

código.py

GALÁXIA EXTRA



Introdução

Olá, seja bem-vindo à Galáxia Extra de AWS, a Amazon Web Service! Neste módulo vamos explorar a maior plataforma de serviços em computação na nuvem, como a automatização de implementação de qualquer algoritmo, aprender a configurar um banco de dados na nuvem e outras diversas coisas mais avançadas. Este é um módulo em que haverá poucas finanças e muita tecnologia envolvida.



Mundo 1

1.1. O que é a Amazon Service Web (AWS)?

Este módulo é o mais complexo do curso, por isso é importante ter paciência e revisar o conteúdo com frequência. É impossível entender tudo de primeira, então não se preocupe se não conseguir.

Na AWS, a sua solução é personalizada para atender às suas necessidades específicas.

A AWS é uma plataforma de computação em nuvem que oferece uma ampla gama de serviços de infraestrutura, como computação, armazenamento, bancos de dados, rede e análise.

A computação em nuvem é uma forma de fornecer serviços de computação, armazenamento, rede e software a partir de servidores remotos, geralmente na internet.

Uma analogia útil para a computação em nuvem é uma lan house. Em uma lan house, você pode alugar um computador por um determinado período de tempo. Você não precisa se preocupar com a manutenção do computador, pois isso é feito pela lan house.

Existem 3 provedores principais: AWS, Azure e Google Cloud. Mas focaremos somente na AWS, pois é a mais utilizada no mundo.

1.2. O que é um servidor?

Um servidor é um computador potente que fornece recursos a outros computadores, como armazenamento, processamento e rede.

As empresas precisam de servidores para executar seus aplicativos e serviços. Os servidores também são usados para fornecer acesso à internet e a outros recursos.

Existem várias vantagens em usar a computação em nuvem em vez de ter um servidor próprio.

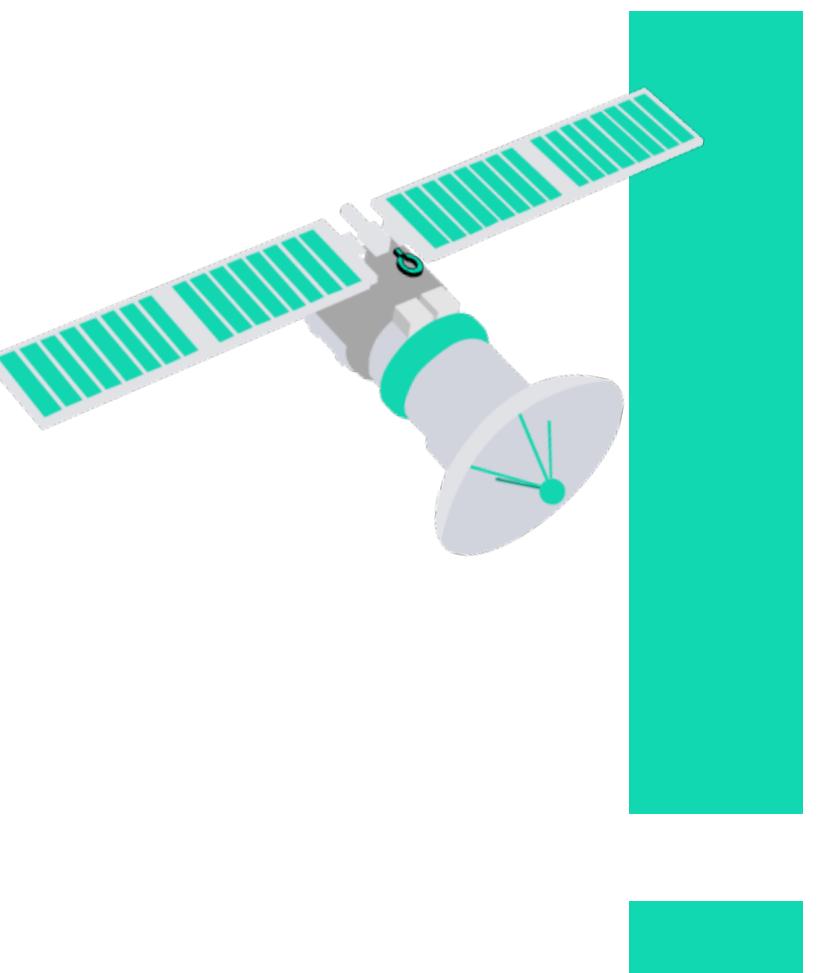
- Flexibilidade: Você pode aumentar ou diminuir o número de servidores que usa de acordo com as suas necessidades. Isso é útil para eventos especiais, como a Black Friday.
- Escalabilidade: Você pode adicionar ou remover recursos de seus servidores conforme necessário. Isso é útil para empresas que crescem ou reduzem de tamanho.
- Redução de custos: A computação em nuvem pode ser mais econômica do que ter um servidor físico próprio.
- Facilidade de uso: A computação em nuvem é mais fácil de usar do que gerenciar um servidor próprio.

Mundo 2

2.1. Principais serviços da AWS?

A AWS oferece uma ampla gama de serviços, mas alguns dos mais populares incluem:

- EC2: Serviço de máquinas virtuais (VMs) que permite criar e gerenciar servidores na nuvem. É como se fosse um computador normal, em que você escolhe a quantidade de RAM, armazenamento, CPU, etc. Adequado para hospedagem de sites, executar sistemas e rotinas pesadas, realizar análise e também rodar modelos de investimento.
- Lambda: Serviço de computação sem servidor que permite executar código através de triggers. Tem também o Serverless, que seria a terceirização da terceirização, onde não é necessário configurar um computador como no EC2, pois a AWS estará encarregada disso. O Lambda é um pouco mais simples que o EC2.



- DynamoDB: Serviço de banco de dados NoSQL que oferece alta escalabilidade e desempenho.
- RDS: Serviço de banco de dados relacional que oferece suporte para uma variedade de sistemas de gerenciamento de banco de dados (RDBMS).
- S3: Serviço de armazenamento de objetos que oferece alta disponibilidade e segurança. É basicamente um HD gigante, um banco de dados de arquivos e sites. Pode ser armazenado até mesmo suas planilhas e parquet.
- API Gateway: Serviço de gateway de API que permite criar e gerenciar APIs.
- IAM: Serviço de gerenciamento de identidade e acesso que permite controlar quem tem acesso aos seus recursos da AWS.
- VPC: Serviço de rede virtual que permite criar redes privadas na nuvem.

Mundo 3

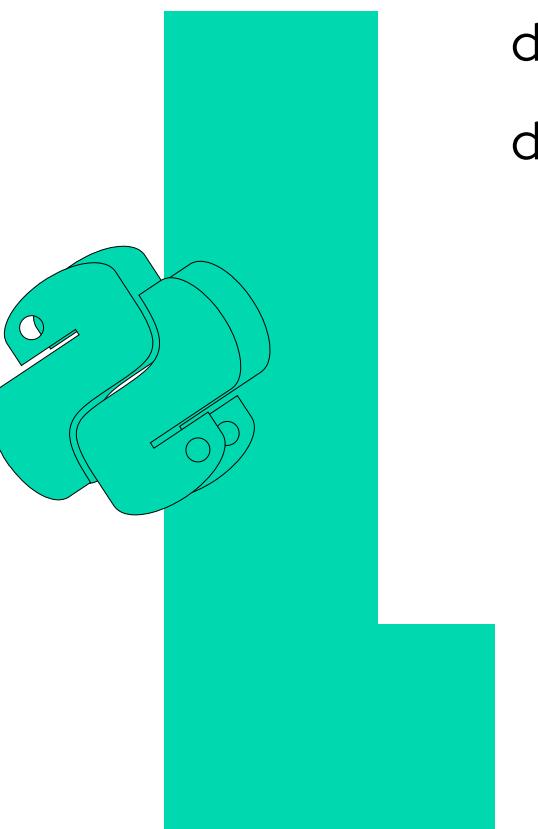
3.1. Zonas de disponibilidade

As zonas de disponibilidade são datacenters físicos separados que estão localizados dentro da mesma região da AWS. Cada zona de disponibilidade é isolada das outras por meio de infraestrutura física e lógica, o que ajuda a garantir a alta disponibilidade e a resiliência dos seus dados.

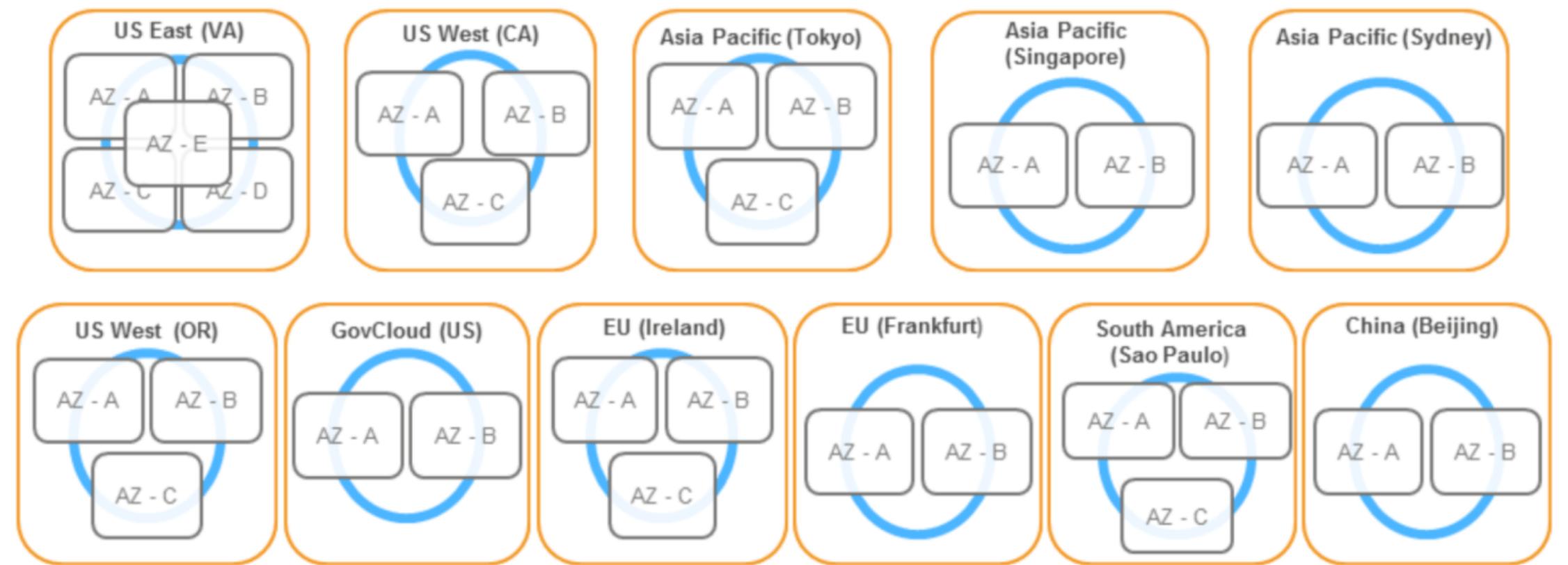


As zonas de disponibilidade devem estar localizadas a um raio de no máximo 100 km umas das outras. Isso é feito para garantir que os dados possam ser replicados entre as zonas de disponibilidade com rapidez e eficiência.

As zonas de disponibilidade também não podem estar muito próximas umas das outras. Isso é feito para evitar que uma única tragédia possa afetar todas as zonas de disponibilidade de uma região, como algum desastre natural.



A AWS replica os seus dados em pelo menos três zonas de disponibilidade diferentes dentro de uma região. Isso significa que, se uma zona de disponibilidade for afetada por uma falha, os seus dados ainda estarão disponíveis nas outras zonas de disponibilidade.



Ao escolher uma região da AWS, você deve levar em consideração o seguinte:

- Preço: O preço dos serviços da AWS varia de acordo com a região.
- Localização: Você deve escolher uma região que esteja próxima aos seus clientes e parceiros.
- Requisitos de conformidade: Você deve escolher uma região que atenda aos seus requisitos de conformidade.

Recomendação: A região us-east-1 é a mais popular da AWS. Ela oferece um bom equilíbrio entre preço, localização e recursos.

Mundo 4

4.1. Integração de códigos na AWS

Console

Essa é a forma visual e manual, você utilizará a interface da AWS diretamente pelo navegador, realizando integrações e configurações de forma prática. Embora seja intuitivo devido à natureza visual, essa abordagem pode se tornar menos eficiente ao programar aplicações. Imagina estar desenvolvendo um script e ter que constantemente alternar entre o código e a interface. Isso pode gerar confusões, com partes do processo na interface e outras no código, dificultando a organização.

É crucial aprender a utilizar a interface da AWS, pois, devido à diversidade de serviços, é natural sentir-se um pouco perdido no início.

CLI

A CLI (Command Line Interface) é uma interface de linha de comando que permite interagir com a AWS por meio de comandos de texto executados em um prompt de comando. Com a CLI, você pode executar as mesmas operações disponíveis no console, mas de forma programática. Esta é a forma mais rápida de se mexer na AWS, ela possui sua própria linguagem.

Imagine o sistema operacional Windows, nele você pode fazer tudo utilizando apenas o mouse por se tratar de um sistema feito para leigos utilizarem. Mas também é possível fazer todos esses comandos por meio de códigos no prompt de comando.

Com a AWS é o mesmo, você pode controlar os serviços da AWS dentro do seu prompt de comando no computador sem precisar abrir a interface dela no navegador.

É por meio da CLI que conectaremos nosso computador à AWS, esta conexão vai nos possibilitar integrar AWS com Python



Boto3

Boto3 é um SDK criado pela AWS que permite que você conecte o Python com AWS de forma segura e rápida. Boto3 foi criado especificamente pro Python, logo você não conseguirá utilizá-lo com outra linguagem de programação.

Um SDK (Software Development Kit) é um conjunto de ferramentas criadas para facilitar a integração, imagine que SDK é uma biblioteca com um conjunto de funções, ou métodos, cada função tem um conjunto de código por trás que foram criados para facilitação do uso.

Qual a diferença entre CLI e Boto3?

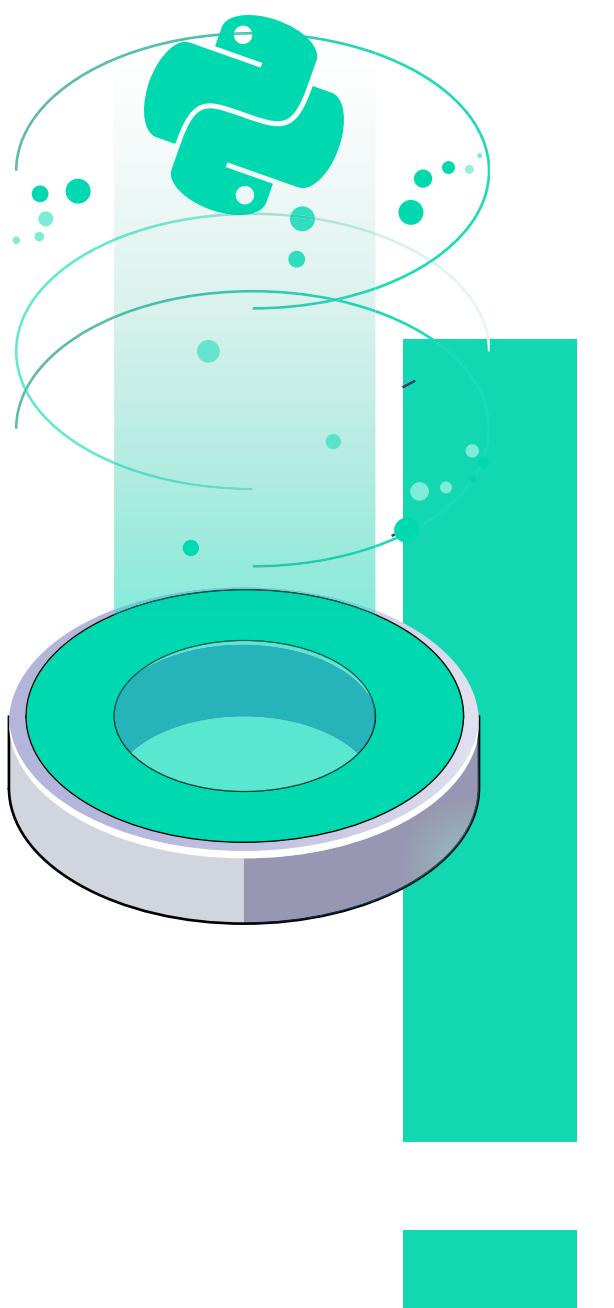
A diferença é que a CLI é utilizada no terminal do computador enquanto o Boto3 é utilizado em um script Python. Imagine que Boto3 é uma biblioteca igual pandas e yfinance, eu conseguiria fazer tudo criando meus próprios métodos do zero, mas para que fazer isso se a AWS disponibiliza esses métodos prontos?

O Boto3 é a forma mais fácil de utilizar o Python com os serviços da AWS, mas para isso você precisará que a CLI esteja conectada ao seu computador, será por meio de chaves secretas que a AWS saberá que a conexão entre sua conta e o seu computador está segura.

É por meio do Boto3 que você conseguirá integrar suas aplicações com os serviços da AWS.

Serverless Framework

O Serverless Framework é um framework de código aberto criado que facilita o desenvolvimento, implantação e gerenciamento de aplicações serverless (sem servidor). Sua proposta é padronizar os comandos de plataformas como AWS, Azure, Google Cloud e etc. Ao invés de você precisar aprender a linguagem de cada plataforma, você só precisaria aprender o serverless framework que faria essa integração diretamente com essas plataformas. Ela faz o mesmo que a CLI, porém de uma forma mais fácil e otimizada. Ela é muito popular entre os desenvolvedores por facilitar a implementação de serviços dentro da AWS de forma padronizada.



Cloudshell

Este não será abordado neste curso, mas é possível também que você mexa na AWS utilizando sua própria linha de comando. Imagine um prompt de comando na interface da AWS.

Qual a diferença entre Cloudshell e CLI?

A diferença é que a CLI é utilizada no seu computador, fora da interface da AWS enquanto o Cloudshell está na interface da AWS e possui sua própria linguagem, assim como o Linux e o Windows.

Mundo 5

5.1. Criando sua conta na AWS

[Serviços de computação em nuvem - Amazon Web Services \(AWS\)](#)

[AWS Console - Signup \(amazon.com\)](#)

Esse link irá direcioná-lo diretamente para a criação da sua conta na AWS. Preencha o campo com as suas devidas informações.

Caso vá utilizar para sua empresa, crie a conta em nome da empresa, e não em nome pessoal. Isso irá facilitar no futuro.

Após essas etapas, cadastre um cartão e fique tranquilo que é impossível gastar US\$10.000. Afinal, a Amazon não quer cobrar nem US\$100 indevidamente, pois isso pode traumatizar e causar perda de clientes. Dentro da AWS, há configurações de teto de gasto para o seu cartão, e também conta free-tier, com os 12 meses iniciais com tudo gratuito.

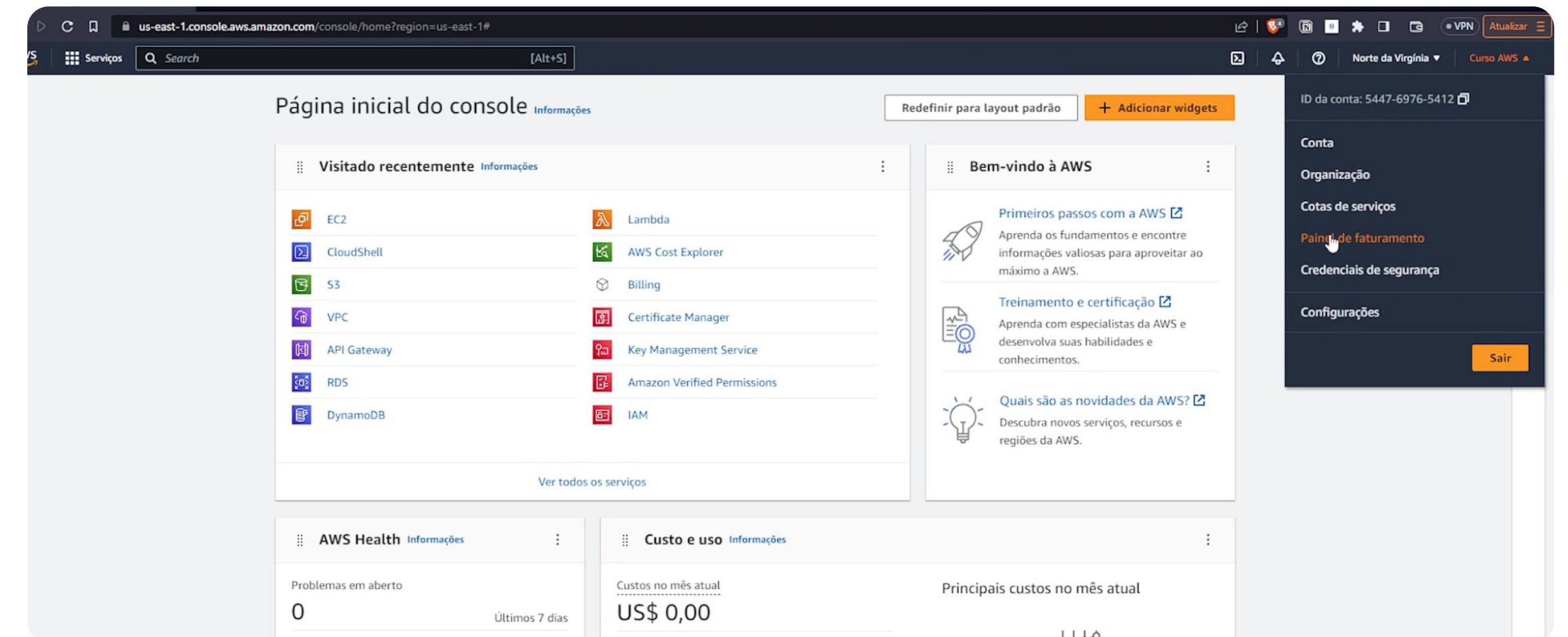
E por fim, selecione o plano gratuito.

Mundo 6

6.1. Controle de gastos

Pode cadastrar o cartão com confiança que este módulo fará você perder o medo através do controle de gastos na AWS.

Todo serviço na AWS é feito sob demanda, portanto, só há cobrança apenas de serviços solicitados/contratados. Lembrando que, após a criação da sua conta, você recebeu o free-tier por 12 meses, com acesso ilimitado a tudo.



Dentro do site, é possível definir o orçamento personalizado que irá te alertar caso exceda o limite de custo, através do AWS Budgets, feito de forma totalmente gratuita. Esse alerta será feito através de e-mail direcionados à você informando coisas do tipo como "Seu limite teve um gasto de 70% até o momento".

The screenshot shows the AWS Budgets landing page. On the left, there's a sidebar with navigation links like 'Faturamento', 'Budgets', and 'Cost explorer'. The main content area features a large 'AWS Budgets' heading with the subtext 'Defina orçamentos personalizados que alertam quando você excede os limites orçados'. Below this is a section titled 'Como funciona' with a flowchart showing the process from 'AWS Budgets' to 'Create a budget', 'Get alerted', and 'Respond with actions'. A prominent orange button labeled 'Criar um orçamento' is at the bottom right of this section.

This screenshot shows the 'Create a budget' configuration page. The sidebar on the left is identical to the previous one. The main area has a section titled 'Budget Type' with two radio button options: 'Orçamento de cobertura diária de Savings Plans' and 'Daily reservation utilization budget'. Below this is a section for 'Orçamento de gasto zero - modelo' where you can enter a name for the budget. Further down are sections for 'Destinatários de e-mail' (Email recipients) and a note about email notifications.

Cost Explorer informa a origem dos gastos, com custos diários em cada serviço, relatórios recém acessados

This screenshot shows the 'Configuração do orçamento' (Budget Configuration) page. It includes sections for 'Usar um modelo (simplificado)' and 'Personalizar (avocado)'. Under 'Modelos - novo', it lists 'Orçamento de gasto zero' (selected), 'Orçamento de custo mensal', 'Orcamento de cobertura diária de Savings Plans', and 'Daily reservation utilization budget'. There's also a section for 'Orçamento de gasto zero - modelo' where you can enter a name. The sidebar on the left includes 'Cost explorer' under 'Cost Management'.

6.2. AWS Pricing Calculation

Talvez você esteja se perguntando sobre o quanto baratos devem ser os serviços da AWS. A própria empresa disponibiliza uma calculadora para isso, a chamada "AWS Pricing Calculation".

Calculadora de preços da AWS (calculator.aws)

Instance name	Categoria da instância	vCPUs	Núcleos físicos	Memória	Network Performance	Armazenamento	On-Demand Hourly Cost	CurrentGeneration	Potencial Effective Hourly Cost (\$Savings %)
t4g.nano	General purpose	2	0.5 GiB	Up to 5 Gigabit	EBS only	0.0042	Yes	0.0016 (63%)	
t3a.nano	General purpose	2	0.5 GiB	Up to 5 Gigabit	EBS only	0.0047	Yes	0.0018 (63%)	
t3.nano	General purpose	2	0.5 GiB	Up to 5 Gigabit	EBS only	0.0052	Yes	0.0019 (63%)	
t2.nano	General purpose	1	0.5 GiB	Low	EBS only	0.0058	Yes	0.0022 (63%)	
t4g.micro	General purpose	2	1 GiB	Up to 5 Gigabit	EBS only	0.0084	Yes	0.0032 (62%)	
t3a.micro	General purpose	2	1 GiB	Up to 5 Gigabit	EBS only	0.0094	Yes	0.0035 (62%)	
t3.micro	General purpose	2	1 GiB	Up to 5 Gigabit	EBS only	0.0104	Yes	0.0039 (62%)	
t2.micro	General purpose	1	1 GiB	Low to Moderate	EBS only	0.0116	Yes	0.0044 (62%)	

As máquinas são divididas em versões, T1, T2, T3 e etc. A T1 é a máquina mais antiga, conforme esses números vão aumentando (T2, T3...) significa que são as versões mais recentes, mais eficientes, gastam menos energia e são mais otimizadas, logo são mais baratas. A AWS já informou que irá substituir as antigas aos poucos.

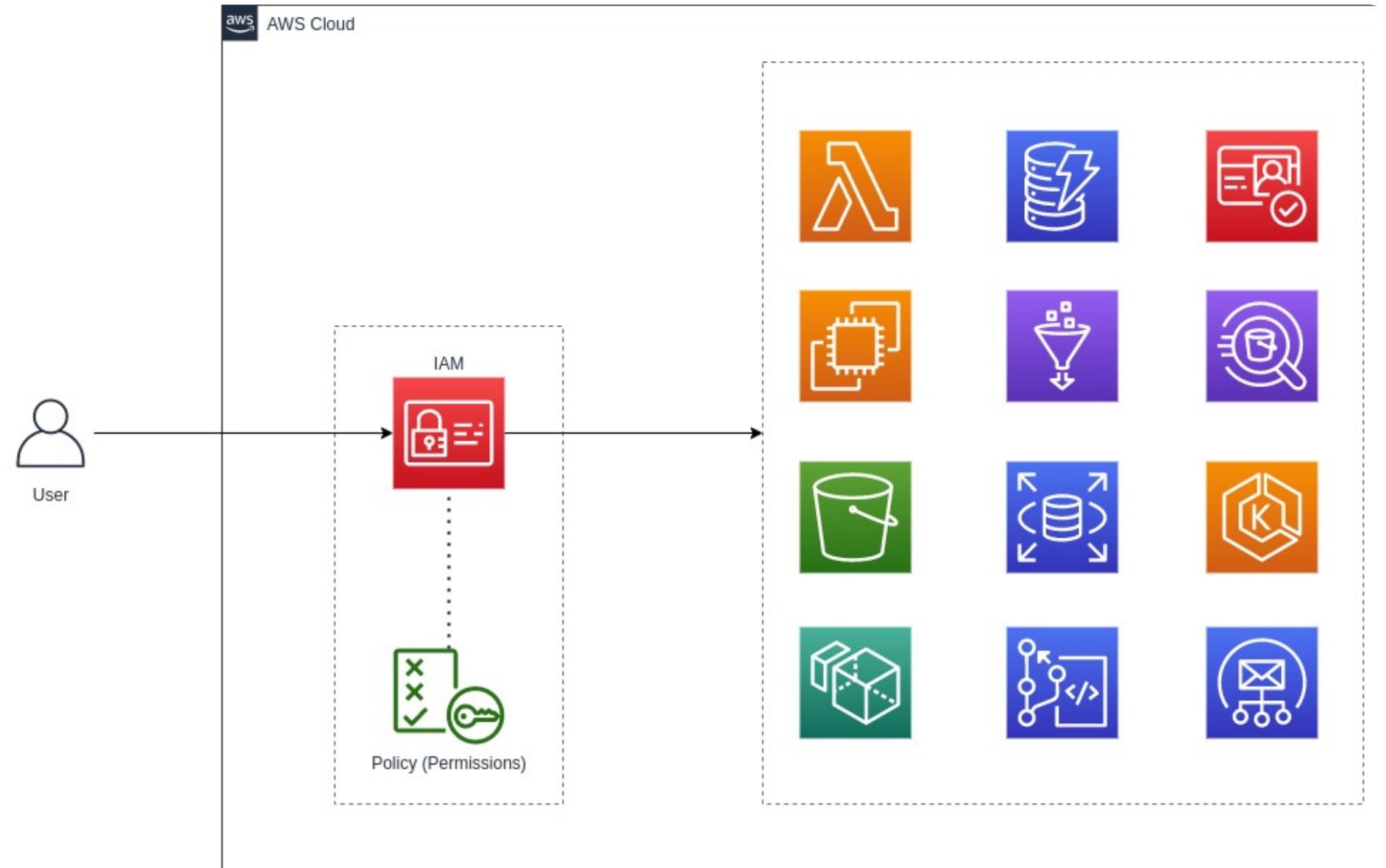
É possível verificar o custo para cada serviço individualmente, busque no google e será redirecionado para alguma página da própria AWS com a tabela das máquinas e valores.

Mundo 7

7.1. Como funciona o IAM?

Essa é a parte que cuida da segurança da AWS, este serviço que define o controle de permissões. Ele é dividido em Groups (Grupos), Users (Usuários), Roles (Funções) e Policies (Políticas). É importante que você saiba como são chamados esses nomes em inglês, pois é assim que eles são conhecidos no meio empresarial, na internet e na documentação.

Todas as ações realizadas na AWS são primeiramente filtradas pelo IAM. Ele é o guardião que concede ou nega acesso aos diferentes serviços. O IAM desempenha um papel crucial na segurança, ajudando a controlar e regular quem tem acesso a quais recursos, promovendo uma gestão mais segura e eficaz dentro da plataforma da AWS.



Definiremos primeiramente o que é cada um e depois exemplificaremos:

1. Políticas (Policies): As políticas são documentos em formato JSON que definem as permissões em relação aos serviços na AWS. Elas especificam o que um usuário, grupo ou função pode fazer. As políticas podem ser anexadas a usuários, grupos ou funções para conceder ou restringir acesso a recursos específicos. Elas desempenham um papel fundamental no controle de acesso dentro do IAM e ajudam a garantir que apenas as ações autorizadas sejam realizadas.

2. Usuários (Users): Usuários representam as identidades individuais que interagem com a AWS, seguindo a boa prática, cada pessoa deve ter seu próprio usuário. Cada usuário tem um nome exclusivo e credenciais de login associadas (geralmente, nome de usuário e senha). Usuários podem ter o acesso limitado através das políticas de acesso atribuídas a eles.

3. Funções (Roles): As funções são identidades que podem ser atribuídas a usuários, serviços ou recursos dentro da AWS. É por meio das funções que você poderá definir permissões temporárias, ou exclusivas, a funcionários ou serviços. Por exemplo, eu posso dar permissões para pessoas sem conta da AWS ou permissão entre os serviços (Já falo sobre).

4. Grupos (Groups): Grupos são coleções de regras definidas que você pode atribuir a um conjunto de usuários. Por exemplo, você pode criar um grupo chamado "Desenvolvedores" e adicionar todos os usuários responsáveis pelo desenvolvimento de aplicativos neste grupo. Em seguida, é possível definir políticas de acesso para o grupo todo, em vez de precisar atribuir permissões individualmente para cada usuário.

Vamos ilustrar como esses conceitos se aplicam na prática:

Imagine que você é o administrador da conta AWS de uma empresa e está contratando novos funcionários. É considerado uma má prática compartilhar um único login entre várias pessoas, pois isso dificulta o rastreamento e monitoramento das ações realizadas.

Para resolver isso, como administrador, você cria novos usuários para cada funcionário, associando a cada um um login exclusivo. Essa prática evita que os funcionários tenham acesso total à conta, algo que é reservado para o administrador, reduzindo a possibilidade de erros ou ações indesejadas.

Agora, imagine que entre esses novos contratados, há um funcionário pleno e dois estagiários. O pleno possui experiência com a interface da AWS, enquanto os estagiários não. Então, dentro do IAM, você cria dois grupos:

Um grupo é designado para o funcionário pleno, concedendo a ele a maioria das permissões necessárias. Enquanto o outro grupo é destinado aos estagiários, fornecendo apenas as permissões mínimas necessárias para suas atividades.

Quanto às funções, imagine que você esteja criando uma máquina virtual na AWS. Por padrão, essa máquina não tem acesso a nenhum outro serviço, pois a AWS preconiza que você conceda as permissões necessárias em vez de conceder acesso total desde o início. Então, você cria uma função específica para essa máquina virtual e a associa a ela. Esse processo é repetido sempre que deseja integrar serviços na AWS.

Por exemplo, se você armazena arquivos em um Bucket no S3, com as devidas permissões, poderá compartilhá-los com qualquer pessoa, mesmo que ela não tenha uma conta na AWS.

As políticas são o ponto inicial para definir quem acessa o quê e quais serviços estão disponíveis. Elas determinam as permissões de acesso para usuários, grupos e funções, garantindo a segurança e a autorização adequada dentro da AWS.

7.2. Acessando a IAM

Entrando na interface da AWS, vá até o campo de busca e digite “IAM” clique no primeiro resultado:

The screenshot shows the IAM dashboard with the following details:

- Security recommendations:**
 - Root user has MFA
 - You have MFA
 - Your user, vinculus_viana, does not have any active access keys that have been unused for more than a year.
- IAM resources:**

User groups	Users	Roles	Policies	Identity providers
0	3	75	40	0
- What's new:**
 - Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023.
 - AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs.
 - AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.
 - Amazon ElastiCache simplifies password rotations with Secrets Manager.

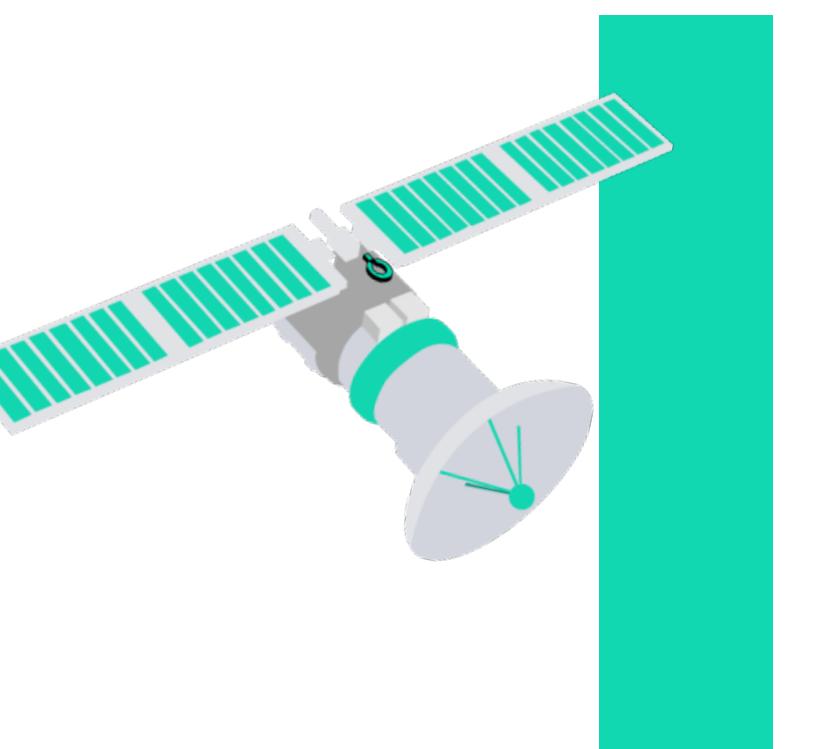
Ao acessar o IAM, a tela principal aparecerá. Inicialmente, é crucial criar um novo usuário, pois usar a conta "root" diariamente aumenta o risco de invasões. A conta "root" possui controle total sobre a conta AWS, sendo suscetível a comprometimentos que podem afetar pagamentos e dados. Criar um usuário separado é uma prática recomendada para atividades mais sensíveis. Ele atua como um "save point" caso o usuário principal seja comprometido.

7.2.1. Criando um novo grupo (Group)

Na aba do lado esquerdo clique em “Grupos de usuários” e depois no canto direito superior clique em “Criar Grupo”.

The screenshot shows the Groups page with the following details:

- Grupos de usuários (0) Informações:** Um grupo de usuários é um conjunto de usuários do IAM. Use grupos para especificar as permissões para um conjunto de usuários.
- Criar grupo:** Button highlighted in red.
- Usuários:** No results.



Você será redirecionado para a seguinte tela abaixo:

1. Dê um nome para o seu grupo

2. No campo de procura digite os textos abaixo, o que queremos é que todos os usuários direcionados a este grupo, tenham todas as permissões que um "root" têm, exceto as de gerenciamento da conta. Então adicionaremos apenas estas duas permissões:

2.1. [AdministratorAccess](#) (Concede acesso de administrador)

2.2. [Billing](#) (Concede acesso ao painel financeiro)

Depois no canto inferior direito clique em "Criar grupo".

Pronto, agora que você já tem seu grupo criado, podemos prosseguir e referenciar esse grupo a algum usuário.

7.2.2. Criando um novo usuário (User)

Na aba do canto esquerdo clique em "Users" e depois no canto superior direito clique em "Add users":

Ao clicar em criar usuários você será redirecionado para seguinte tela, onde:

Especificar detalhes do usuário

Detalhes do usuário

Nome do usuário 1

Fornecer acesso para os usuários ao Console de Gerenciamento da AWS - opcional 2

Você está fornecendo acesso ao console para uma pessoa?

Quero criar um usuário do IAM 3

Senha do console

Senha gerada automaticamente 4

Mostrar senha

Os usuários devem criar uma nova senha no próximo login (recomendado) 5

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 6

[Cancelar](#) [Próximo](#)

1. Será o nome do usuário.

2. Você definirá se o acesso do usuário que você está criando será de forma programática ou se ele vai ter acesso ao gerenciamento da conta, por meio da interface da AWS, que necessitará de um login. O acesso de forma programática é por meio de chaves de autenticação e esse acesso só pode ser feito através da API ou CLI. Ou seja, não tem acesso a interface AWS. Então deixaremos essa opção marcada para permitir que este usuário tenha acesso à conta e consequentemente ao Login.

3. Seleccione a opção “crie um usuário do IAM”, que nada mais é do que, um usuário no qual determinaram quais permissões ele teria.

4. Escolha a opção que desejar, eu escolherei a opção de que a senha seja criada automaticamente.

5. Escolha a opção de que o dono do usuário criará uma nova senha no primeiro Login.

6. Vá a próxima página.

Avançando para a próxima página, podemos adicionar esse usuário que estamos criando em um grupo com as permissões já definidas criado anteriormente. O bom de associar usuários a um grupo é que quando precisar mudar as permissões desses usuários é só mudar a permissão do grupo que afetará automaticamente todos os usuários deste grupo.

Podemos copiar as permissões já definidas à um usuário anteriormente:

E por último, definir nossas próprias permissões, assim como fizemos ao criar um grupo. Contudo, não é necessário adicionar um usuário a um grupo, você pode anexar políticas diretamente a eles. Porém, a melhor prática é criar um grupo e adicionar essas políticas a este grupo. Exceto se, sejam políticas bem específicas.

Ao avançar para a próxima página, iremos tratar de Tags.

The screenshot shows the 'Review and create' step of the IAM user creation wizard. It displays the user details and summary of permissions. The 'Tags' section, which allows adding key-value pairs to the user, is highlighted with a red box. This section includes fields for 'Chave' (Key) and 'Valor - opcional' (Optional Value), along with a 'Remover' (Remove) button and a link to 'Adicione uma nova etiqueta' (Add a new tag). Navigation buttons 'Cancelar' (Cancel), 'Anterior' (Previous), and 'Criar usuário' (Create user) are at the bottom.

As etiquetas (Tags) têm funções importantes no contexto de organização, sendo elas:

1. Organização: As etiquetas ajudam a organizar e categorizar os recursos da AWS. Por exemplo, você pode adicionar etiquetas para indicar a finalidade de um recurso, o ambiente em que está sendo usado, o proprietário ou a equipe responsável por ele. Isso facilita a identificação e a gestão dos recursos.

2. Faturamento e alocação de custos: As etiquetas podem ser usadas para atribuir custos a projetos, equipes ou departamentos específicos em uma organização. Elas são úteis para identificar o consumo de recursos e auxiliam na análise e alocação de custos.

3. Automação e gerenciamento: As etiquetas são amplamente utilizadas para automatizar tarefas de gerenciamento de recursos na AWS. Por exemplo, você pode criar políticas baseadas em etiquetas para controlar o acesso aos recursos, definir alarmes com base em determinadas etiquetas ou até mesmo automatizar ações com base em condições específicas de etiquetas.

4. Identificação e rastreamento: As etiquetas permitem identificar e rastrear recursos em um ambiente complexo e em constante mudança. Elas fornecem informações adicionais que podem ser usadas para pesquisar e filtrar recursos com base em critérios específicos.

Mas, não iremos adicionar etiqueta no momento, portanto, crie o usuário, e será redirecionado para a próxima página.



7.3. Criando uma nova função

Por fim, criaremos uma função (role). Diferentemente dos casos acima, este recurso pode ser associado a outros serviços da AWS. É ele que dará a permissão necessária para que seus serviços façam integrações entre si. Por padrão, a AWS não disponibiliza essas permissões como “full access” de primeira, é você que tem que escolher quais recursos podem acessar o que.

Há a possibilidade também de que outra conta AWS possa acessar sua Bucket, será por meio de funções também. Mas o caso de maior uso é entre os serviços.

Vá até a página do IAM e clique em “Funções” no canto esquerdo e depois em “Criar Função”:

Imagine que você tenha uma máquina virtual no serviço EC2, para que essa máquina virtual acesse o seu Bucket ela precisará das permissões necessárias e através das funções que você dará essa possibilidade.

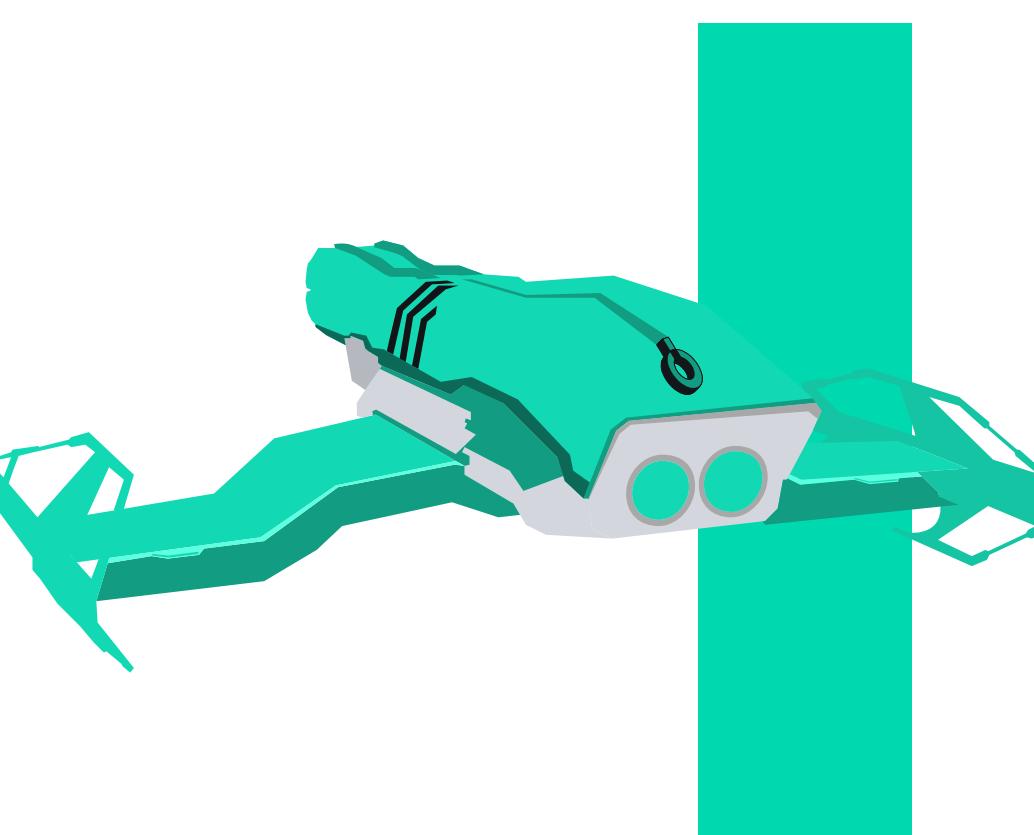
Assim que você for redirecionado para página abaixo, você terá as opções de:

1. Escolher entre serviços da AWS, outras contas da AWS entre outros. Escolha Serviços.
2. Abaixo você terá que escolher qual serviço quer, como você quer dar permissão para uma máquina virtual acessar uma Bucket, você precisará escolher o serviço “EC2”:

3 - Clique em próximo para seguir a página

Nesta página, daremos apenas o acesso ao S3, pesquise pelo "AmazonS-
3FullAccess", selecione e prossiga:

Crie um nome para sua função e finalize.



7.4. Logando na AWS

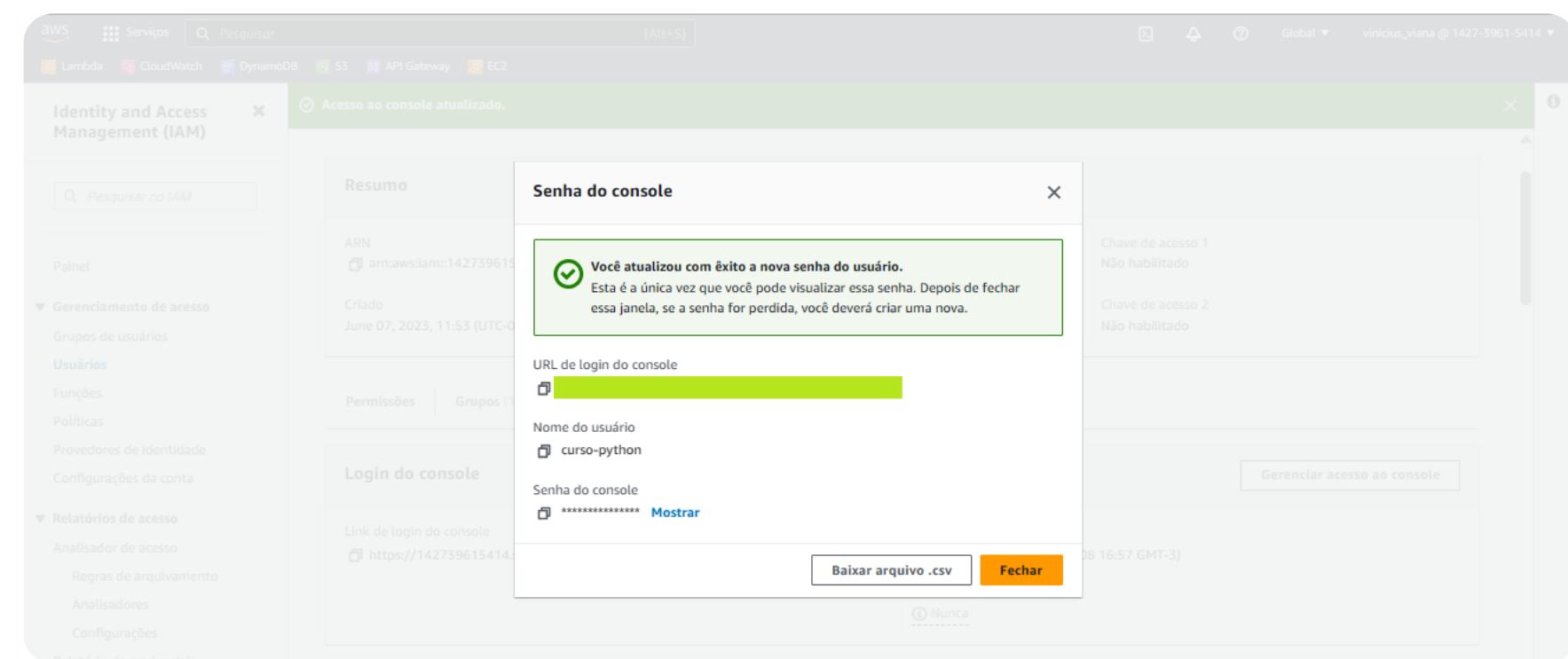
Na página inicial do IAM, escolha a conta:

The screenshot shows the AWS IAM service's 'Users' section. There are two users listed: 'curso-python' and 'curso-python-programatico'. The 'curso-python' user is highlighted with a red box. The interface includes a search bar, a toolbar with buttons like 'Adicionar usuário', and a sidebar with navigation links for IAM.

Direcionado para a próxima página, siga esta sequência.

The screenshots show the process of enabling AWS console access for a user. Step 1 shows the 'Credenciais de segurança' tab selected in the IAM 'Resumo' page. Step 2 shows the 'Gerenciar acesso ao console' dialog with the 'Habilitar' checkbox checked. Step 3 shows the same dialog with the 'Senha gerada automaticamente' checkbox checked. Both dialogs include a note about the IAMUserChangePassword policy.

Colha as informações e realize o login através do link, mas lembre-se de baixar o arquivo csv, pois assim que você acessar o link não poderá mais entrar na sua conta AWS.



Agora, para finalizar as configurações, ative o MFA.



7.5. Ativando o MFA

MFA é uma verificação por 2 fatores, sendo crucial para a segurança da sua conta AWS, e é imprescindível que seja ativado. Vá na aba do IAM e clique em "Ativar MFA":

Mundo 8

8.1. O que é S3?

S3 significa Simples Storage Service, e foi o primeiro serviço criado pela AWS. Sua função é o armazenamento de arquivos.

Ao criar sua conta, você ganha um Free Tier de 5 GB por 12 meses na AWS para usar no S3, é um período gratuito que a AWS fornece para teste, depois desses 12 meses a AWS inicia a cobrança.

No S3, como mencionado no mundo 2, você pode salvar absolutamente tudo que você quiser: parquet, planilhas, pdfs, arquivos, sites, qualquer coisa que você precise ter acesso rápido. Devido às integrações da AWS, fica muito fácil fazer download e upload dos arquivos no S3. É claro que a integração é muito melhor quando se usa serviços da AWS, já que eles conversam muito bem entre si, porém serviços de fora também podem se conectar ao S3, mas com menos facilidade e rapidez.

Alguns exemplos de como usar o S3:

- Armazenamento de arquivos estáticos de sites: os arquivos, como imagens, CSS e JS, são armazenados no S3 e servidos pelo site por URLs geradas pelo S3.
- Backup de banco de dados: o S3 é usado para armazenar backups de bancos de dados, permitindo uma rápida recuperação em caso de falhas ou perda de dados.
- Armazenamento de arquivos de logs: os arquivos de logs gerados por aplicações podem ser armazenados no S3, permitindo uma fácil consulta e análise.
- Streaming de vídeos e músicas: o S3 é utilizado para armazenar arquivos de vídeos e músicas que são transmitidos para os usuários em tempo real.

Todos esses arquivos são salvos em uma Bucket, utilizamos esse nome "Bucket" para referenciar um espaço onde os arquivos ficarão salvos. Você pode criar quantas Buckets quiser e colocar quantos dados quiser, contudo, é bom que você diferencie-as. O nome escolhido para Bucket tem que ser único em sua região. Ao criar sua Bucket, atente-se à região criada, pois ela estará disponível somente na região selecionada.

Para explicar detalhadamente sobre a criação de uma bucket, é necessário o entendimento sobre classes de armazenamento.



8.2. Classes de armazenamento

Existem classes diferentes dentro do S3 que definem uma Bucket, isso porque como tudo dentro da AWS é feito sob demanda, a AWS entende que deve cobrar mais de um Bucket que é recorrentemente acessada. Afinal, uma Bucket que é acessada recorrentemente precisa estar armazenada em discos mais rápido, como SSD's, por exemplo.

Pense que você tem um programa que acessa imagens diariamente em um Bucket S3 e disponibiliza em um site. Este acesso precisa ser de alta velocidade com o menor tempo possível.

Em contrapartida, você pode ter um Backup em uma Bucket que só será acessado em casos de emergência, ou talvez nem seja acessado.

Por isso a AWS criou as classes de armazenamento, é ela que definirá onde serão armazenados seus arquivos.

Na documentação você encontra detalhadamente para que serve cada uma e os preços, que costumam variar em cada região.

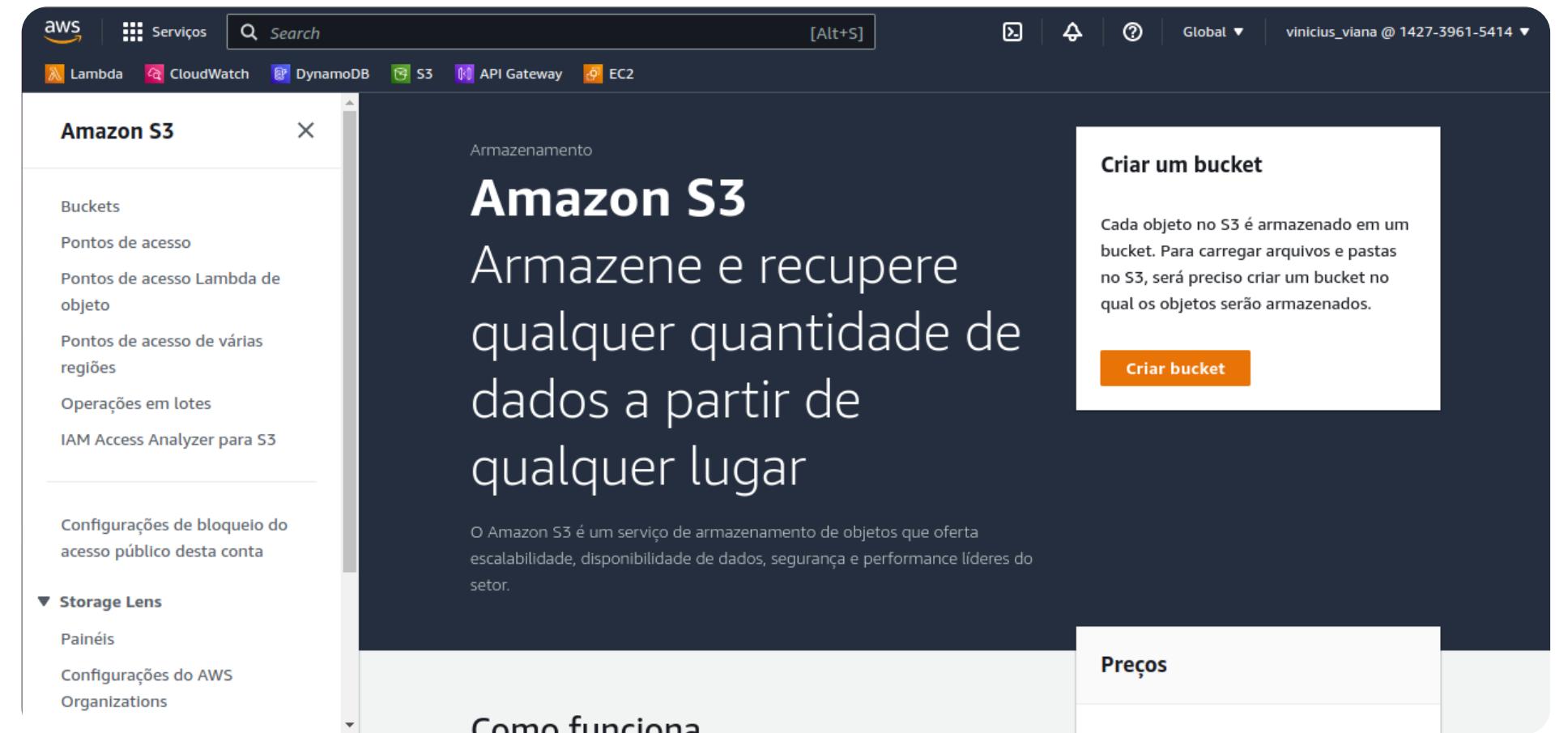
[Classes de armazenamento de objetos – Amazon S3](#)

8.3. Quais os valores?

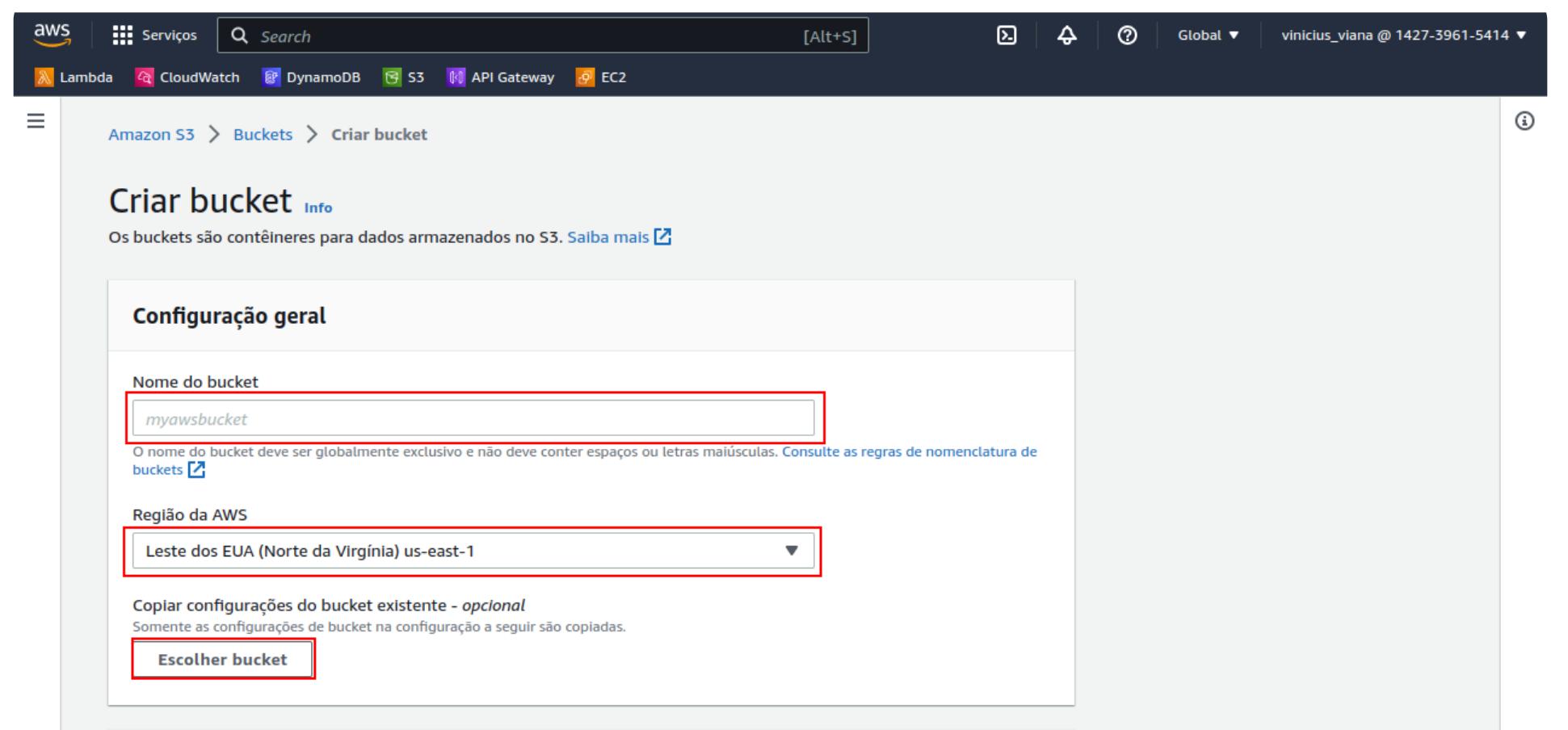
Na AWS, é disponibilizado o valor de cada serviço ([Preço Amazon S3 - AWS](#)), mas o melhor jeito seria utilizar a própria calculadora da AWS ([AWS Pricing Calculator](#)). É importante que você saiba que existe um custo para modificar a classe de um Bucket. Por isso é bom que você esteja bem atento ao criar uma Bucket.

8.4. Bucket

Para criar uma bucket você vai precisar ir até a página inicial do S3. Vá até este painel e clique em “Criar Bucket”.



Escolha um nome que seja único na sua região, escolha a região.



Escolha se a ACL (Access List) será habilitada ou não. A partir da ACL é definido quem pode visualizar os objetos dentro do Bucket. Se um Bucket for criado com a ACL desabilitada, ela não poderá ser habilitada novamente. Por isso, habilite a ACL e depois defina quem pode ou não acessar seu Buckets.

Propriedade de objeto [Info](#)

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.

Propriedade do objeto
Imposto pelo proprietário do bucket

Esta função definirá quem poderá acessar os objetos dentro da Bucket. Por padrão, esta função vem como “blockeada ao acesso público”. Quando for liberar o acesso ao público, certifique-se que não há dados sensíveis. E lembre-se, você não paga por criar uma Bucket, e sim pela quantidade de dados que utilizar.

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Assim como o GitHub, o S3 suporta versionamento de objetos. Em resumo, toda vez que você altera, adiciona ou sobrepõe um arquivo é gerado um commit, que nada mais é do que um histórico de cada etapa do seu Bucket. Esse recurso é utilizado quando precisamos retornar a uma versão antiga. Ao habilitar esteja ciente que este serviço pode gerar custos adicionais, pois a cada commit ele guarda uma “duplicata” do seu arquivo. Isso pode acontecer centenas de vezes.... Você pode se deparar com 100 versões diferentes do mesmo arquivo, por exemplo. É claro que, estes commits só serão criados caso haja uma diferença nos arquivos, você não terá 100 versões do mesmo arquivo, por exemplo.

Versionamento de bucket

O versionamento é um meio de manter múltiplas variantes de um objeto no mesmo bucket. Você pode usar o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. Com o versionamento, você pode recuperar facilmente ações não intencionais do usuário e falhas da aplicação. [Saiba mais](#)

Versionamento de bucket

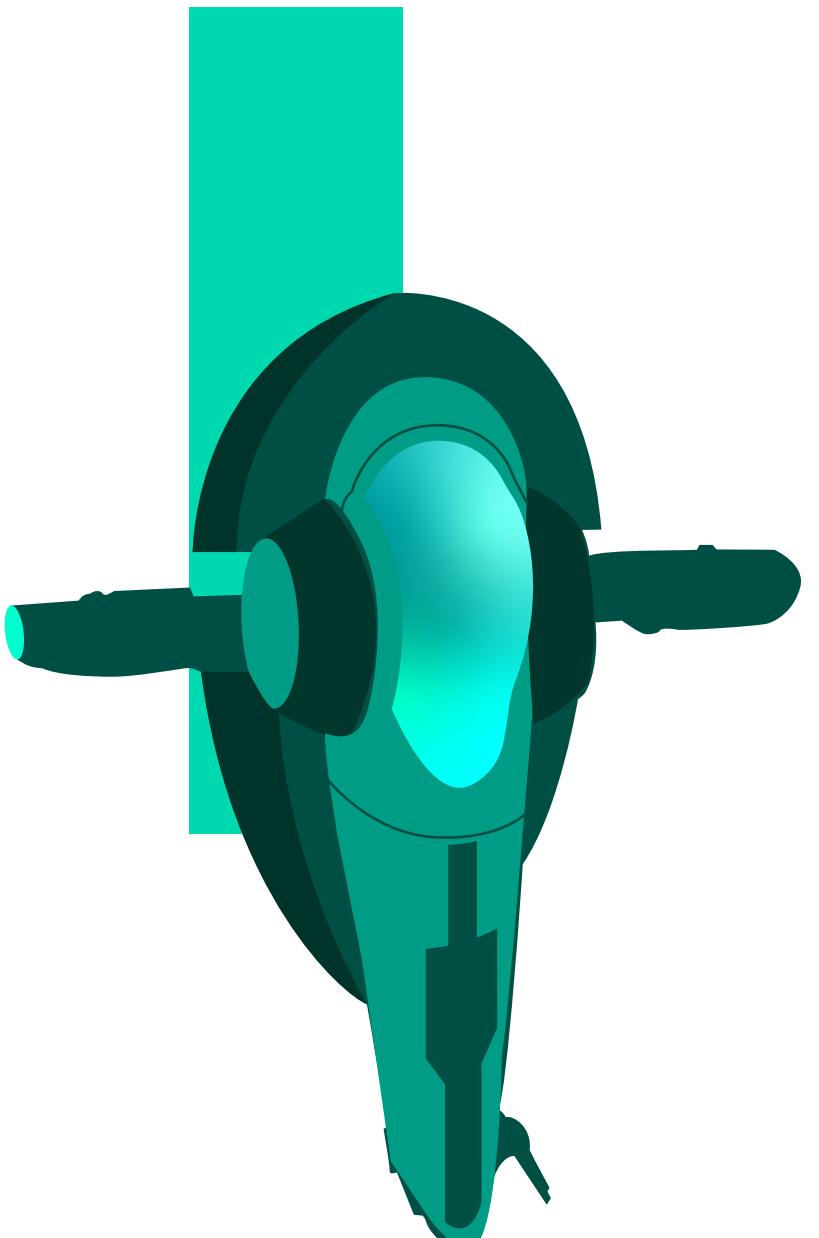
Desativar
 Ativar

A Tag foi explicada no mundo 7, e é ótima para organizar e gerar métricas.

A criptografia que fará a segurança da sua Bucket, existem alguns tipos de criptografia no S3, mas não fará muita diferença para você. Só que é importante que você saiba como elas funcionam:

SSE-S3 (Server Side Encryption - S3): Significa que a criptografia está sendo feita dentro da Bucket no S3 e gerenciada pela própria S3. Ao fazer upload de um arquivo ele só será criptografado quando este estiver dentro da Bucket, ele estará “desprotegido” o restante do caminho percorrido até a Bucket. O processo inverso funciona quando houver download do arquivo de uma Bucket, ele será descriptografado antes de sair da Bucket e fará o resto do caminho “desprotegido”.

SSE-KMS (Server Side Encryption - KMS): O mesmo funciona para esta opção, a diferença é que neste caso o serviço será gerenciado pelo KMS



Criptografia padrão Informações
A criptografia no lado do servidor é aplicada automaticamente a novos objetos armazenados nesse bucket.

Tipo da chave de criptografia Informações
 Chaves gerenciadas pelo Amazon S3 (SSE-S3) Chave do AWS Key Management Service (SSE-KMS)

Chave do bucket
Quando a criptografia do KMS é usada para criptografar novos objetos nesse bucket, a chave do bucket reduz os custos de criptografia ao reduzir as chamadas para o AWS KMS. [Saiba mais](#)

Desativar Ativar

▼ Configurações avançadas

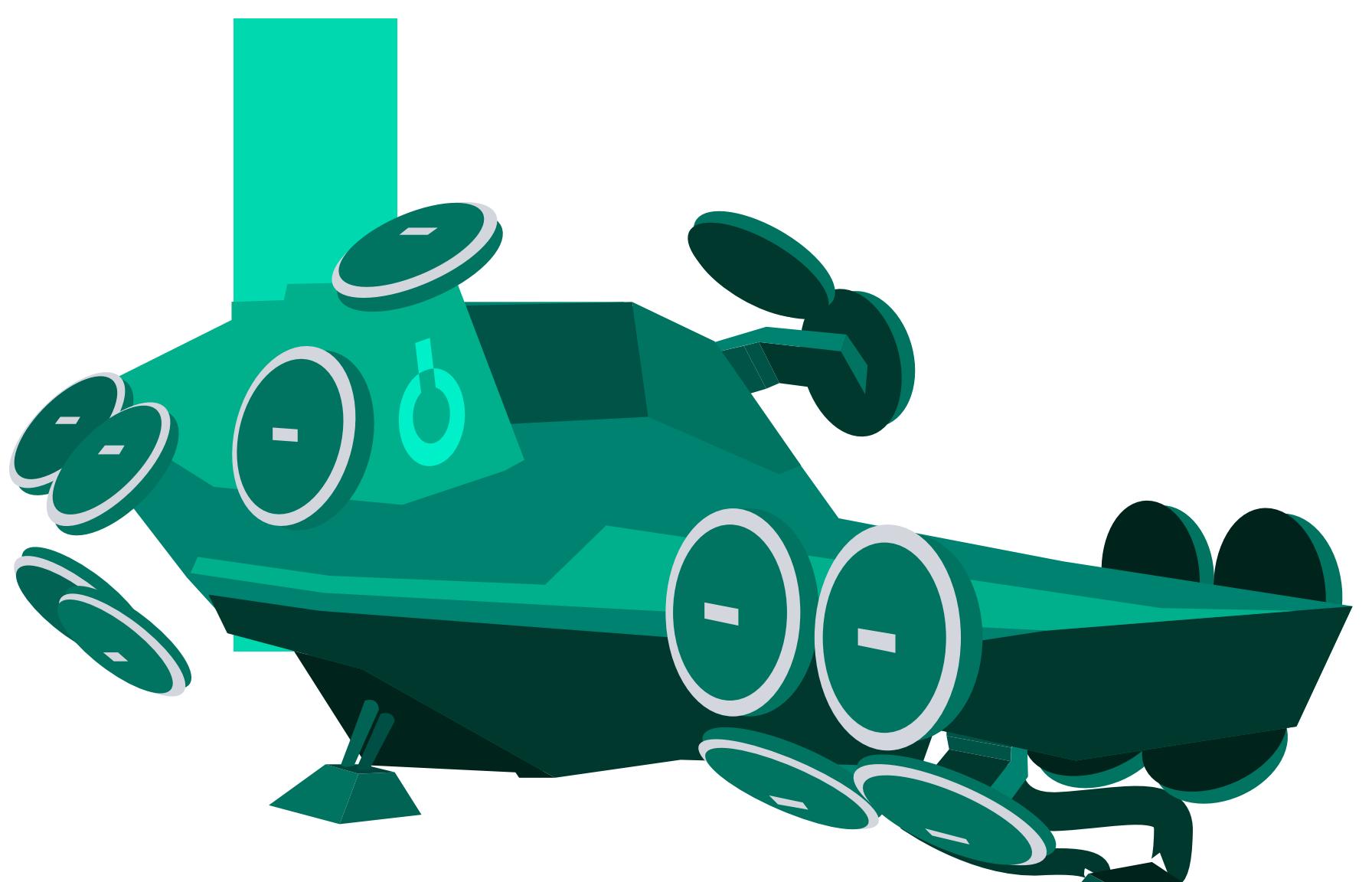
Bloqueio de objeto
Armazene objetos usando um modelo write-once-read-many (WORM - uma gravação, várias leituras) para ajudar a evitar que objetos sejam excluídos ou substituídos por um período fixo ou indefinidamente. [Saiba mais](#)

Desativar Ativar
Permite sempre que os objetos neste bucket sejam bloqueados. Será necessário usar uma configuração adicional nos detalhes do bucket após sua criação para proteger os objetos contidos nele contra exclusão ou substituição.

💡 O bloqueio de objetos só funciona em buckets com versionamento. A habilitação do bloqueio de objetos habilita automaticamente o versionamento de bucket.

Após essa etapa, crie seu bucket e procure por ele.

The screenshot shows the AWS S3 buckets list. At the top, there's a search bar with 'Q. bucket-teste' and a result count of '1 correspondência'. Below the search bar, there are columns for 'Nome', 'Região da AWS', 'Acesso', and 'Data de criação'. A single bucket is listed: 'bucket-teste-curso-copy' located in 'Leste dos EUA (Norte da Virgínia) us-east-1' created on '13 Jun 2023 10:59:18 AM -03'. The 'Criar bucket' button is visible at the bottom right of the list area.



8.4.1. Propriedades da Bucket

Nesta seção, será explicado todas as propriedades acerca do Bucket.

The screenshot shows the 'Propriedades' tab of the AWS S3 bucket 'bucket-teste-curso-copy'. The page is divided into several sections: 1. Visão geral do bucket: Shows the region as 'Leste dos EUA (Norte da Virgínia) us-east-1', ARN as 'arn:aws:s3:::bucket-teste-curso-copy', and creation date as '13 Jun 2023 10:59:18 AM -03'. 2. Versionamento de bucket: Shows 'Desabilitado'. 3. Tags: Shows 'Tags (0)' and 'Nenhuma tag associada a este recurso.' 4. Criptografia padrão: Shows 'Desabilitado'. Red numbers 1, 2, 3, and 4 are overlaid on these sections respectively.

The screenshot shows the 'Properties' tab of an AWS S3 bucket named 'intelligent-tiering'. The configuration is divided into several sections:

- Configurações do Intelligent-Tiering Archive (0)**: Shows a table with columns 'Nome', 'Status', 'Escopo', 'Dias até a transição para o nível Archive Access', and 'Dias até a transição para o nível Deep Archive Access'. A red box highlights the first row, labeled 5.
- Registro em log de acesso ao servidor**: Shows a table with columns 'Nome', 'Status', and 'Descrição'. A red box highlights the first row, labeled 6.
- Eventos de dados do AWS CloudTrail**: Shows a table with columns 'Nome', 'Acesso', and 'Dados'. A red box highlights the first row, labeled 7.
- Notificações de eventos (0)**: Shows a table with columns 'Nome', 'Tipo de evento', 'Filtros', 'Tipo de destino', and 'Destino'. A red box highlights the first row, labeled 8.
- Amazon EventBridge**: Shows a table with columns 'Nome', 'Status', and 'Descrição'. A red box highlights the first row, labeled 9.
- Transfer Acceleration**: Shows a table with columns 'Nome', 'Status', and 'Descrição'. A red box highlights the first row, labeled 10.
- Bloqueio de objeto**: Shows a table with columns 'Nome', 'Status', and 'Descrição'. A red box highlights the first row, labeled 11.
- Pagamento pelo solicitante**: Shows a table with columns 'Nome', 'Status', and 'Descrição'. A red box highlights the first row, labeled 12.
- Hospedagem de site estático**: Shows a table with columns 'Nome', 'Status', and 'Descrição'. A red box highlights the first row, labeled 13.

Seção 1: São as informações sobre a sua Bucket

Seção 2: Sobre o versionamento

Seção 3: Sobre as Tags

Seção 4: Sobre a criptografia

Por mais que essas propriedades já tenham sido definidas antes, você pode editá-las a qualquer momento clicando no botão de "Editar".

Seção 5: O Intelligent-Tiering define por conta própria em qual classe seu objeto deveria estar, caso ele esteja ativado é claro. Por exemplo: Imagine que você tenha acessado muitas vezes um objeto em um mês e depois simplesmente não o acessou mais, o "Intelligent-Tiering" vai definir que ao invés de uma classe padrão, esses arquivos poderiam estar em uma classe mais barata, por exemplo. É um recurso muito importante que vale a pena ser habilitado.

Seção 6: Esta seção é de bastante importância também, ela permite que os logs de quem acessou o seu Bucket sejam salvos, inclusive o seu, ou seja, esses dados e informações de cada pessoa que viu as informações que estavam no seu Bucket.

Seção 7: Esta seção trata sobre a integração do S3 com outro serviço da AWS, o CloudTrail, com esta integração você conseguirá dados mais detalhados sobre quem acessou o seu Bucket e claro que você terá um custo adicional por isso.

Seção 8: Esta seção também trata sobre a integração do S3 com outros serviços da AWS, como SQS e NSS, com esta integração você conseguirá gerar mensagens sempre que acontecer alguma coisa com a sua Bucket.

Por exemplo: Imagine que você queira enviar um email sempre que algum arquivo novo entrar na sua Bucket no S3, será por meio desta integração. Sendo que pode ter também de uma aplicação ser iniciada por isso, não se prenda apenas ao envio de mensagem.

Seção 9: Esta seção também trata sobre a integração do S3 com outros serviços da AWS, como SQS e NSS, com esta integração você conseguirá gerar mensagens sempre que acontecer alguma coisa com a sua Bucket.

Seção 10: Para acessar transferências para outra região da AWS, muito utilizado para projetos grandes em escala global.

Seção 11: Para bloquear alterações em projetos salvos no seu Bucket, para garantir que a primeira versão está íntegra.

Seção 12: Esta seção é para habilitar que pessoas que accessem esse Bucket sejam responsáveis pelos próprios custos de acesso, por exemplo. Pessoas anônimas não poderão acessar o seu Bucket.

Seção 13: Este serviço é utilizado para armazenar um site dentro da S3. Você deve ter cuidado pois a AWS cobra por acessos e requisições, então isso pode gerar custos adicionais caso o site seja bastante acessado.

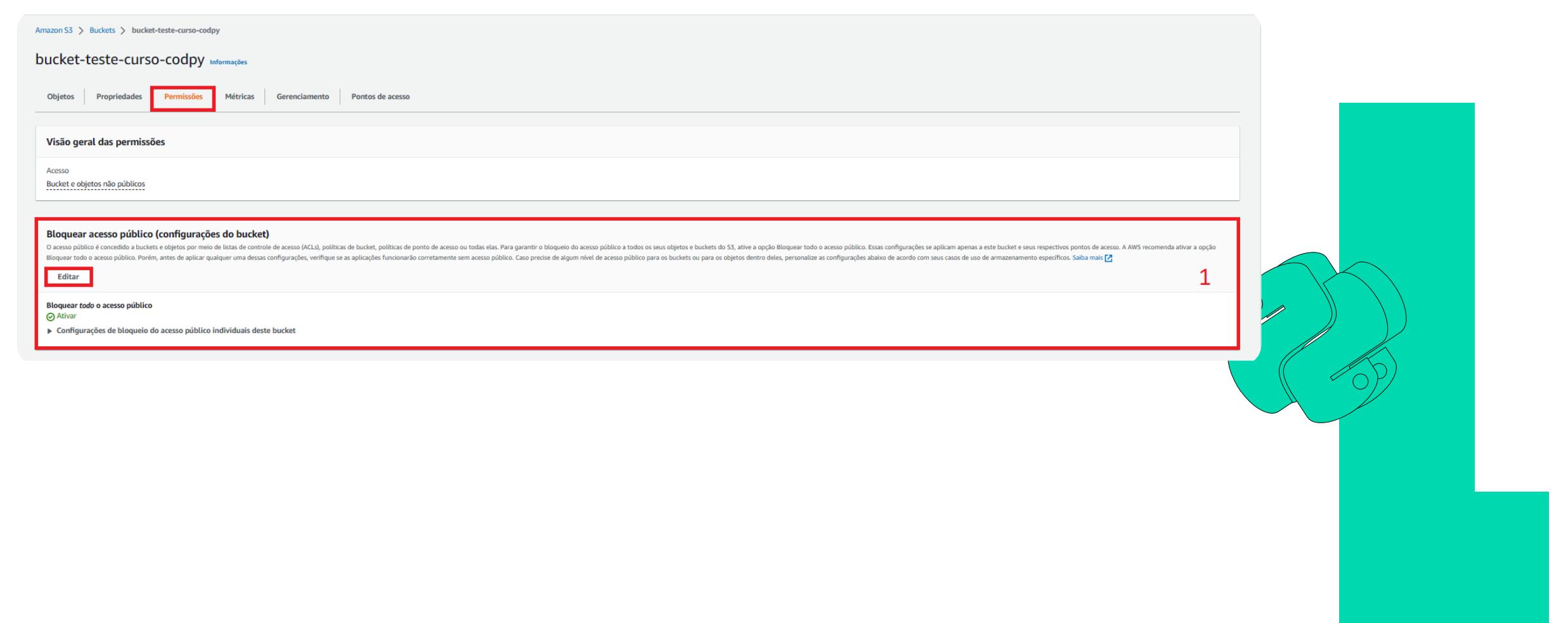
Além da seção de “Propriedades” há uma apenas para as “Permissões”, é esta seção responsável pelos acessos da sua Bucket.

8.4.2. Permissões da Bucket

Seção 1: Esta primeira seção vai definir quem pode acessar sua Bucket. Como podemos ver, ela está bloqueada para todos os públicos, ou seja, só você tem acesso a ela.

8.4.2.1. Liberando o acesso à Bucket

Clicando em editar, você vai se deparar com esta tela:



E assim, você irá definir quem pode acessar sua Bucket, existem várias opções, escolha a mais adequada conforme sua necessidade.

Amazon S3 > Buckets > bucket-teste-curso-copy >
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.

[Cancelar](#)

[Salvar alterações](#)

Seção 2: Assim como IAM, em uma Bucket posso estabelecer políticas. Sua formatação por debaixo dos panos é no formato Json, mas a AWS também disponibiliza uma interface para que você faça suas próprias políticas.

Seção 3: Esta seção definirá se a ACL's serão habilitadas ou não.

Política do bucket

O acesso público é bloqueado porque as configurações de Bloquear acesso público estão ativadas para este bucket.

Nenhuma política a ser exibida.

Propriedade do objeto

Propriedade do objeto

Imposto pelo proprietário do bucket

Seção 5: CORS (Cross-Origin Resource Sharing) é uma especificação que permite que recursos, como fontes de fontes ou scripts, sejam solicitados de um domínio para outro. O S3 suporta CORS, o que significa que você pode especificar qual origem tem permissão para acessar seus objetos S3. É uma configuração importante a ser feita quando você precisa permitir que um site externo accesse seus arquivos no S3.

Lista de controle de acesso (ACL)

Esse bucket tem a configuração imposto pelo proprietário do bucket aplicada à propriedade do objeto.

Beneficiário

Proprietário do bucket (sua conta da AWS)

Objetos

ACL do bucket

Beneficiário

Todos (acesso público)

Grupo: http://acs.amazonaws.com/groups/global/AllUsers

Grupo de usuários autenticados (qualquer pessoa com uma conta da AWS)

Grupo: http://acs.amazonaws.com/groups/global/AuthenticatedUsers

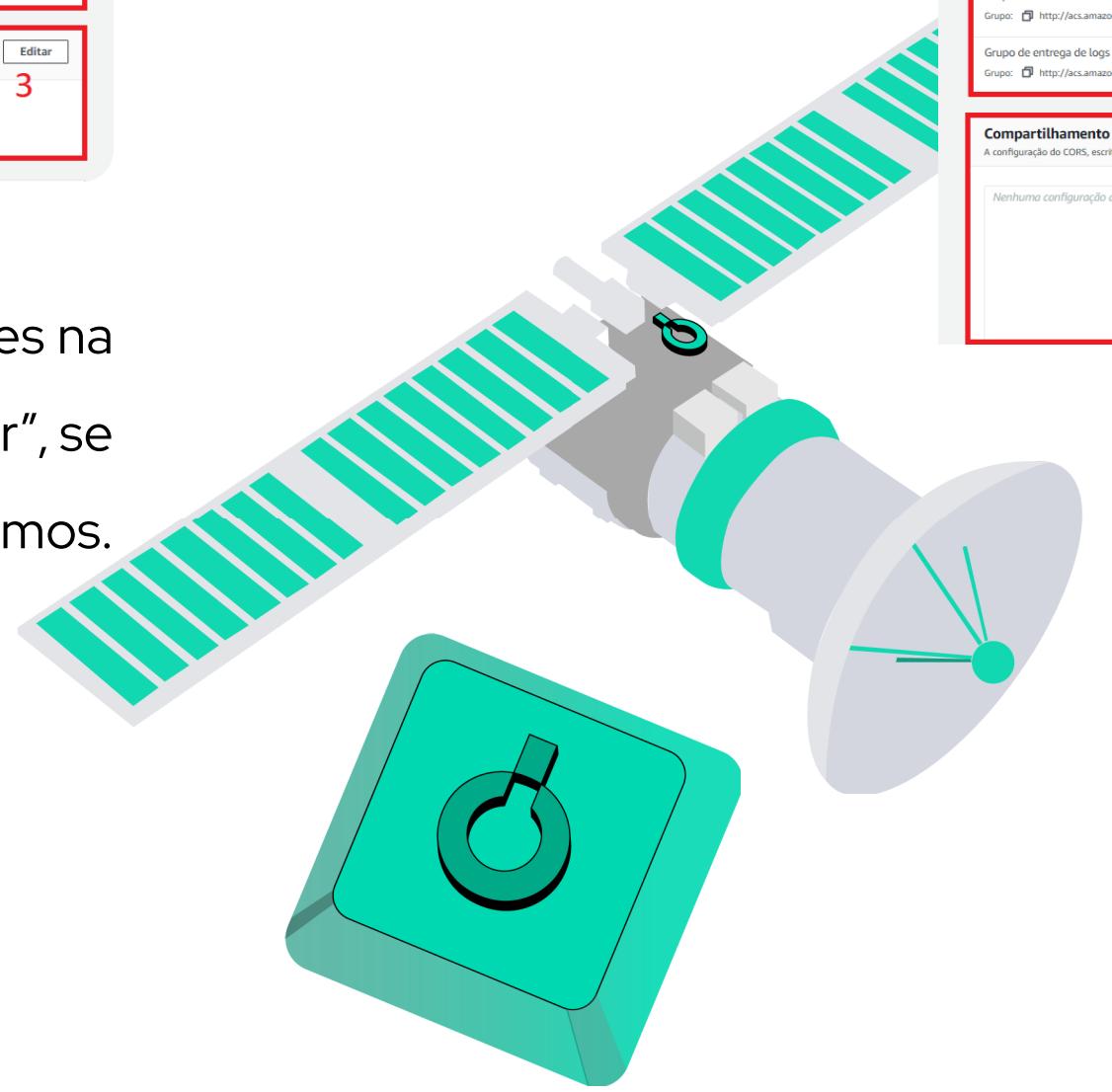
Grupo de entrega de logs do S3

Grupo: http://acs.amazonaws.com/groups/s3/LogDelivery

Compartilhamento de recursos de origem cruzada (CORS)

Nenhuma configuração a ser exibida.

Seção 4: Esta seção vai definir as propriedades das contas AWS presentes na Access List. Mas como a ACL esta desabilitada a gente não consegue “editar”, se estivesse habilitada a gente poderia dar permissões a grupos que preferíssemos.



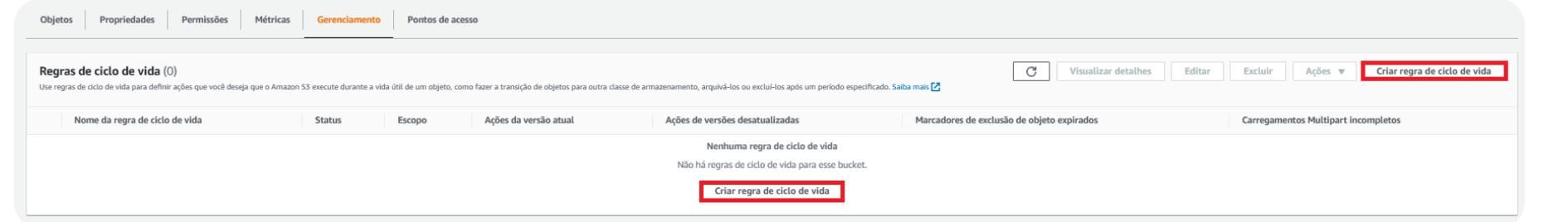
8.4.3. Métricas do Bucket

Na aba de “Métricas” podemos visualizar as métricas do Bucket, como ele é novo não há nada por aqui:

8.4.4. Gerenciamento do Bucket

Na aba de “Gerenciamento” poderemos criar algumas regras que nos ajudam a administrar nossos arquivos automaticamente.

Seção 1: Nesta seção podemos criar regras que façam com que arquivos que não foram mexidos nos últimos 3 dias sejam mudados de classes ou até mesmo excluídos. Podemos criar regras como manter apenas a última versão do versionamento, etc.



Criar regra de ciclo de vida

Configuração da regra de ciclo de vida

Nome da regra de ciclo de vida
Inserir nome da regra
Até 255 caracteres

Escolha um escopo de regra
 Limitar o escopo desta regra usando um ou mais filtros
 Aplicar a todos os objetos no bucket

Aplicar a todos os objetos no bucket
Se você deseja que a regra se aplique a objetos específicos, você deve usar um filtro para identificar tais objetos. Escolha "Limitar o escopo desta regra usando um ou mais filtros". [Saiba mais](#)

Reconheço que esta regra se aplicará a todos os objetos no bucket.

Ações de regras de ciclo de vida
Escolha as ações que você deseja que esta regra execute. Taxas por solicitação se aplicam. [Saiba mais](#) ou consulte a [definição de preço do Amazon S3](#)

- Mover versões atuais de objetos entre classes de armazenamento
- Mover versões desatualizadas de objetos entre classes de armazenamento
- Excluir versões atuais de objetos
- Excluir permanentemente versões desatualizadas de objetos
- Excluir marcadores de exclusão de objetos expirados ou carregamentos fracionados incompletos

Essas ações não têm suporte ao filtrar por etiquetas de objetos ou tamanho de objeto.

Analizar ações de transição e expiração

Ações da versão atual	Ações de versões desatualizadas
Dia 0 Nenhuma ação definida.	Dia 0 Nenhuma ação definida.

[Cancelar](#) **Criar regra**

Seção 2: Nesta seção podemos criar regras para gerenciar arquivos entre regiões automaticamente. Pode ser utilizado em projetos que estão em diferentes regiões.

Seção 3: Este serviço fornece relatórios detalhados sobre os objetos e metadados armazenados em seu bucket do Amazon S3. Os relatórios incluem informações como tamanho, criador, data de criação, última atualização e classe de armazenamento. O inventário pode ser gerado em vários formatos, incluindo CSV, ORC, Parquet e Avro. Você pode escolher o formato que melhor se adapta às suas necessidades.



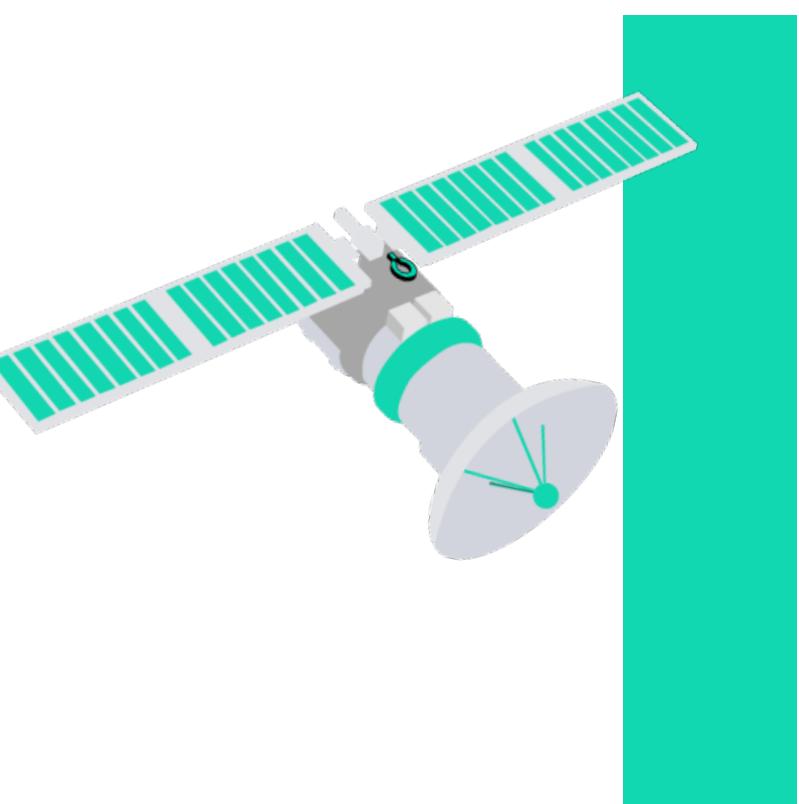
8.4.5. Pontos de acesso da Bucket

Um ponto de acesso S3 é um recurso específico no serviço Amazon S3 que simplifica o acesso e o gerenciamento de dados em um Bucket do S3. Em vez de usar o nome do Bucket como parte da URL para acessar os objetos, você pode criar um nome de domínio personalizado para o seu Bucket usando um ponto de acesso. Isso facilita a organização e o acesso aos objetos armazenados no Bucket.

Aqui estão algumas situações em que você pode usar pontos de acesso S3:

1. Organização de acesso: Se você tiver vários aplicativos ou equipes que precisam acessar diferentes partes do seu Bucket do S3, os pontos de acesso permitem criar URLs separadas para cada um deles. Isso ajuda a organizar e isolar o acesso aos dados, evitando conflitos e confusões.

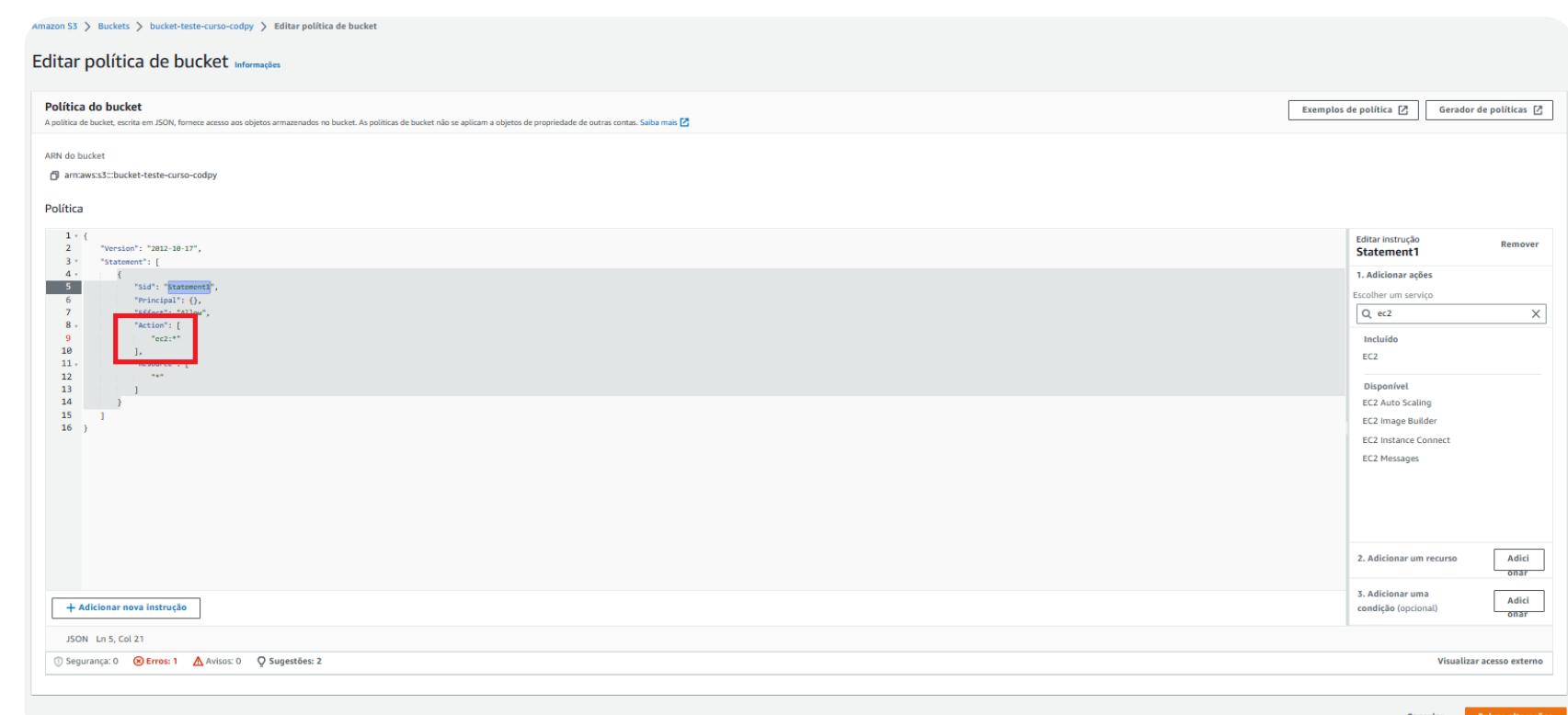
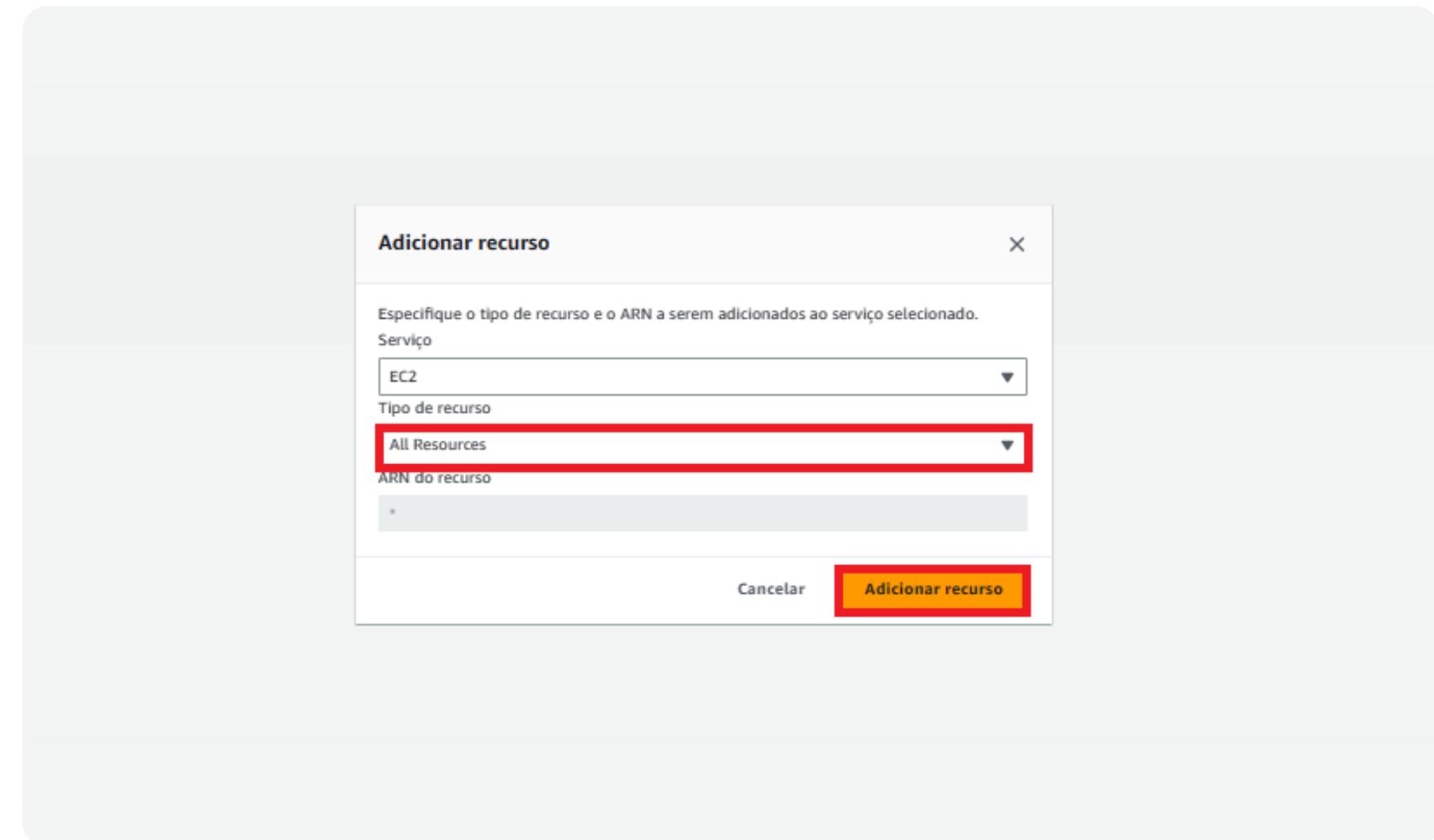
2. Controle de acesso granular: Os pontos de acesso S3 permitem aplicar políticas de controle de acesso granular em diferentes partes do Bucket. Isso significa que você pode definir permissões específicas para diferentes prefixos de objeto ou tags. Por exemplo, você pode permitir que um aplicativo acesse apenas objetos com um determinado prefixo ou que uma equipe específica tenha permissão de leitura/gravação em objetos com uma determinada tag. Isso simplifica o gerenciamento de permissões e melhora a segurança dos dados.



8.4.6. Associando permissões à Bucket

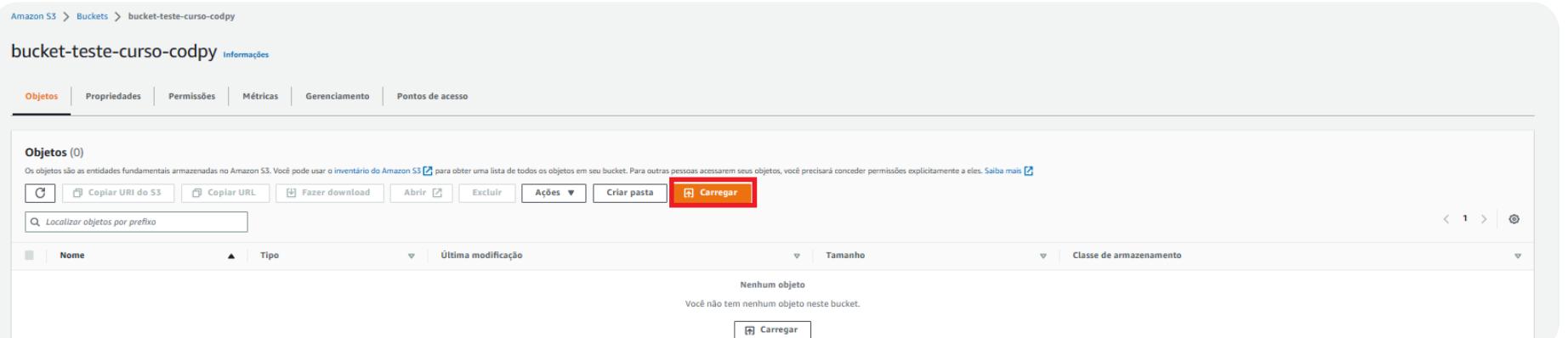
Nesta seção, aprenderá a gerar as permissões de acesso do Bucket.

Digite o nome do serviço para ter acesso à sua Bucket, selecionamos EC2 para este caso.



É assim que se pode definir permissões em uma Bucket, só não se esqueça que existem outras maneiras de atribuir as permissões, como usuários e roles.

8.4.7. Adicionando arquivo na Bucket



Amazon S3 > Buckets > bucket-teste-curso-copy > Carregar

Carregar Informações

Adicione os arquivos e pastas que você deseja carregar no S3. Para fazer upload de um arquivo maior que 160 GB, use a AWS CLI, o SDK da AWS ou a API REST do Amazon S3. Saiba mais [\[?\]](#)

Arraste e solte aqui os arquivos e pastas para upload ou escolha Adicionar arquivos ou Adicionar pastas.

Arquivos e pastas (0) Remover Adicionar arquivos Adicionar pasta

Todos os arquivos e pastas desta tabela serão carregados.

	Nome	Pasta	Tipo	Tamanho
Nenhum arquivo ou pasta Você não escolheu qualquer arquivo ou pasta para carregar.				

Destino

Destino [s3://bucket-teste-curso-copy](#)

Detalhes do destino

Configurações de bucket que afetam novos objetos armazenados no destino especificado.

Versionamento de bucket

Quando habilitado, várias variantes de um objeto podem ser armazenadas no bucket visando facilitar a recuperação de ações não intencionais do usuário e falhas da aplicação. [Saiba mais \[?\]](#)

Desabilitado

Tipo de chave de criptografia padrão

Se uma chave de criptografia não for especificada, as configurações de bucket para a criptografia padrão serão usadas para criptografar objetos ao armazená-los no Amazon S3. [Saiba mais \[?\]](#)

Chaves gerenciadas pelo Amazon S3 (SSE-S3)

Bloqueio de objeto

Quando habilitado, é possível impedir a exclusão ou a substituição dos objetos neste bucket por um período fixo ou indefinidamente. [Saiba mais \[?\]](#)

Desabilitado

Permissões

Conceda acesso público e acesso a outras contas da AWS.

Propriedades

Especifique classe de armazenamento, configurações de criptografia, tags e muito mais.

CANCELAR **Carregar**

Arquivos e pastas (0) Remover Adicionar arquivos Adicionar pasta

Todos os arquivos e pastas desta tabela serão carregados.

	Nome	Pasta	Tipo	Tamanho
Nenhum arquivo ou pasta Você não escolheu qualquer arquivo ou pasta para carregar.				

Nesta parte a gente pode alterar algumas das configurações do destinatário, que no nosso caso é o nosso Bucket.

Destino

Destino [s3://bucket-teste-curso-copy](#)

Detalhes do destino

Configurações de bucket que afetam novos objetos armazenados no destino especificado.

Versionamento de bucket

Quando habilitado, várias variantes de um objeto podem ser armazenadas no bucket visando facilitar a recuperação de ações não intencionais do usuário e falhas da aplicação. [Saiba mais \[?\]](#)

Desabilitado

Tipo de chave de criptografia padrão

Se uma chave de criptografia não for especificada, as configurações de bucket para a criptografia padrão serão usadas para criptografar objetos ao armazená-los no Amazon S3. [Saiba mais \[?\]](#)

Chaves gerenciadas pelo Amazon S3 (SSE-S3)

Bloqueio de objeto

Quando habilitado, é possível impedir a exclusão ou a substituição dos objetos neste bucket por um período fixo ou indefinidamente. [Saiba mais \[?\]](#)

Desabilitado

Habilitar versionamento de bucket

Recomendamos que você habilite o versionamento de bucket para ajudar a proteger contra substituição ou exclusão involuntária de objetos. [Saiba mais \[?\]](#)

Podemos definir as "Permissões" também, no nosso caso ele impossibilita, pois estamos com acesso ao público bloqueado.

Em “Propriedades”, podemos escolher a classe de armazenamento que o arquivo será salvo e definir outras configurações que foram ensinadas até esse momento.

Classe de armazenamento

O Amazon S3 oferece uma variedade de classes de armazenamento projetadas para diferentes casos de uso. Saiba mais ou consulte a definição de preço do Amazon S3.

Classe de armazenamento	Projetado para	Zonas de disponibilidade	Duração mínima de armazenamento
<input checked="" type="radio"/> Padrão	Dados acessados com frequência (mais de uma vez por mês) com acesso a milissegundos	≥ 3	-
<input type="radio"/> Intelligent-Tiering	Dados com padrões de acesso alterados ou desconhecidos	≥ 3	-
<input type="radio"/> Padrão-IA	Dados acessados com pouca frequência (uma vez por mês) com acesso a milissegundos	≥ 3	30 dias
<input type="radio"/> Uma zona-IA	Dados recarregáveis e acessados com pouca frequência (uma vez por mês) armazenados em uma única zona de disponibilidade com acesso a milissegundos	1	30 dias
<input type="radio"/> Recuperação instantânea do Glacier	Dados de arquivamento de longa duração acessados uma vez por trimestre com recuperação instantânea em milissegundos	≥ 3	90 dias
<input type="radio"/> Glacier Flexible Retrieval (o antigo Glacier)	Dados de arquivamento de longa duração acessados uma vez por ano com recuperação de minutos para horas	≥ 3	90 dias
<input type="radio"/> Glacier Deep Archive	Dados de arquivamento de longa duração acessados menos de uma vez por ano com recuperação de horas	≥ 3	180 dias
<input type="radio"/> Redundância reduzida	Dados não críticos, acessados com frequência, com acesso a milissegundos (não recomendados porque o S3 Standard é mais econômico)	≥ 3	-

Criptografia no lado do servidor [Informações](#)
A criptografia no lado do servidor protege dados em repouso.

Não especificar chave de criptografia
As configurações de bucket para criptografia padrão são usadas para criptografar objetos ao armazená-los no Amazon S3.

Especificar chave de criptografia
A chave de criptografia especificada é usada para criptografar objetos antes de os armazenar no Amazon S3.

Aviso: Se a política de bucket exigir que os objetos sejam criptografados com uma chave de criptografia específica, você deverá especificar a mesma chave de criptografia ao carregar objetos. Caso contrário, os uploads falharão.

somas de verificação adicionais
Use função de soma de verificação para a verificação de integridade de dados adicionais de novos objetos. [Saiba mais](#)

Desativar
Quando desabilitado, o Amazon S3 usa uma combinação de somas de verificação MD5 e ETags para verificar a integridade dos dados.

Ativar
Quando habilitado, é possível especificar uma função de soma de verificação para a validação de integridade de dados adicionais.

Tags - opcional
Você pode usar tags de objeto para analisar, gerenciar e especificar permissões para objetos. [Saiba mais](#)

Nenhuma tag associada a este recurso.
[Adicionar tag](#)

Metadados - opcional
Metadados são informações opcionais fornecidas como um par de nome-valor (chave-valor). [Saiba mais](#)

Nenhum metadado associado a este recurso.
[Adicionar metadados](#)

Por fim, é só apertar em “Carregar”.

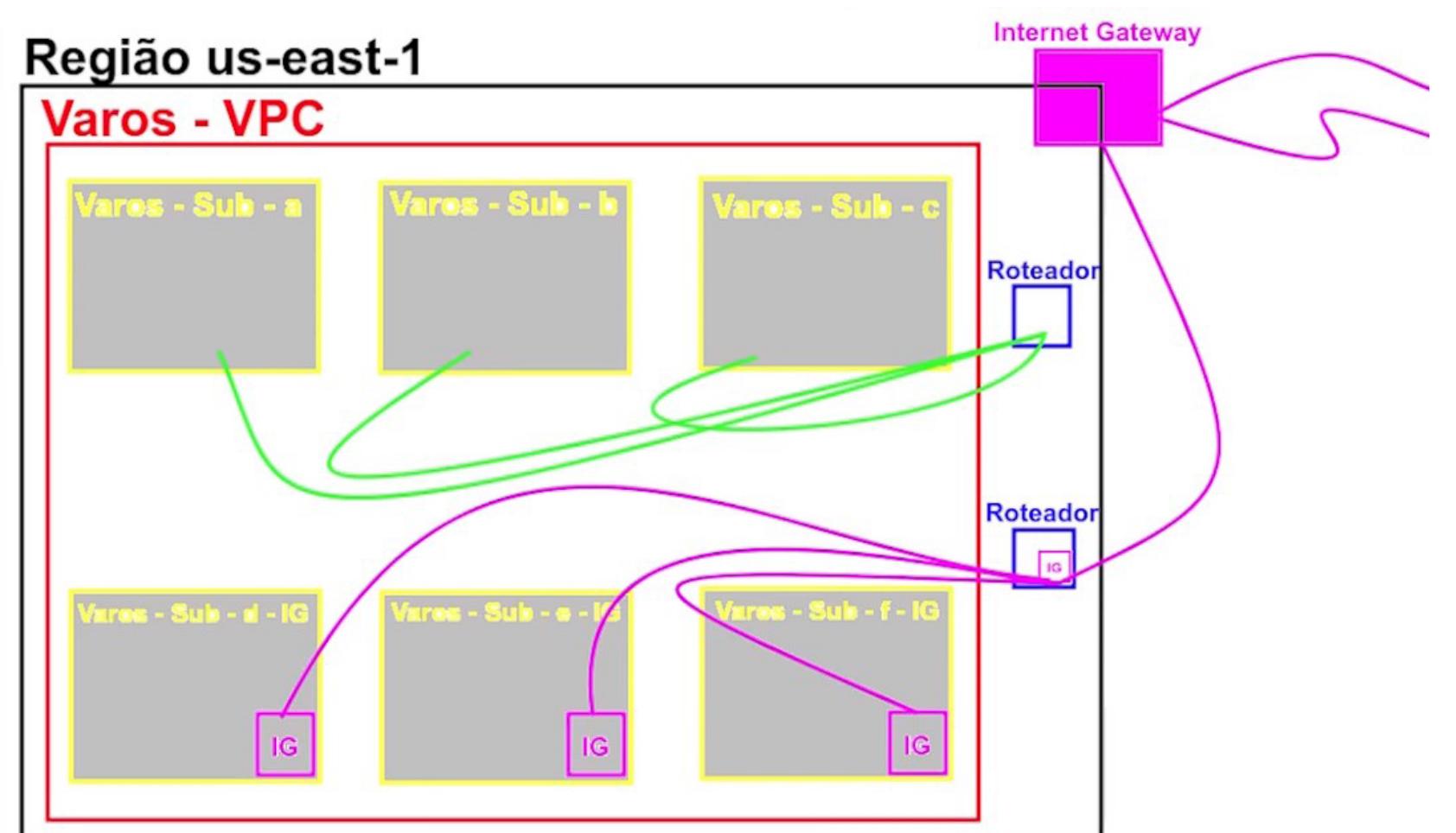
Mundo 9

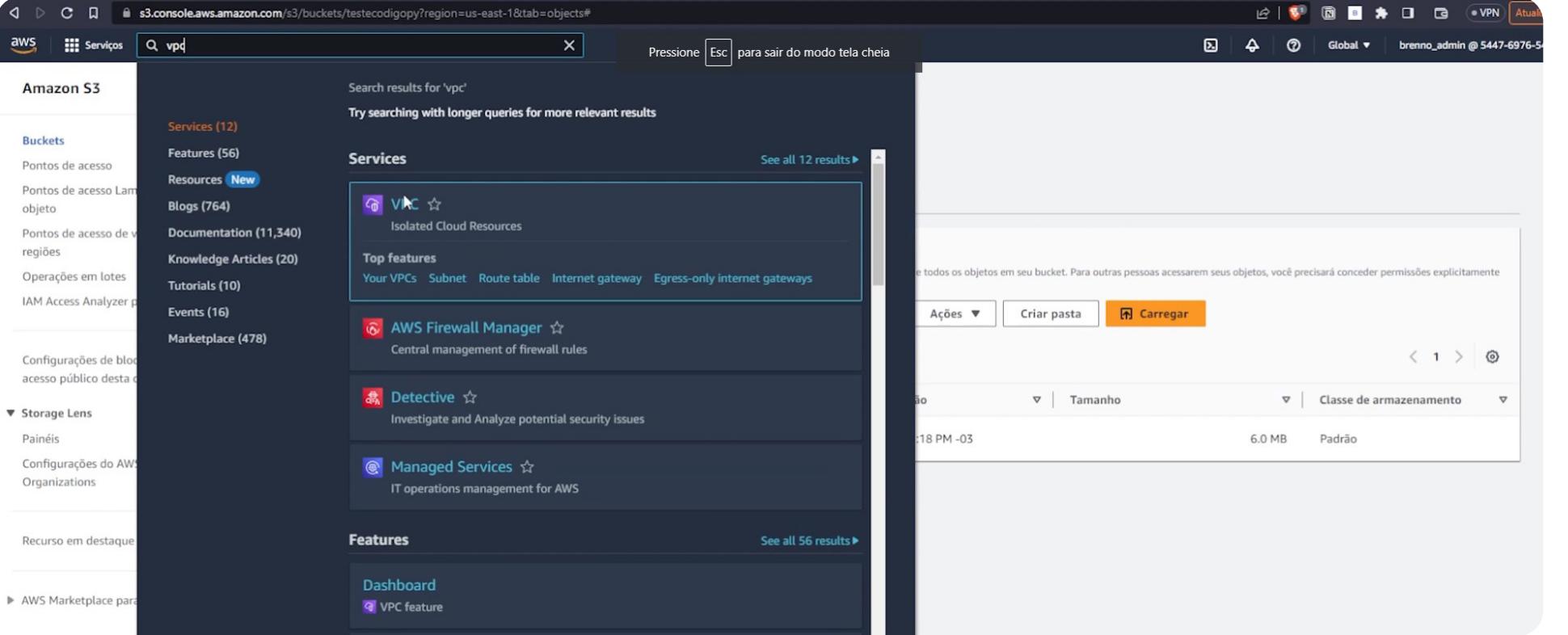
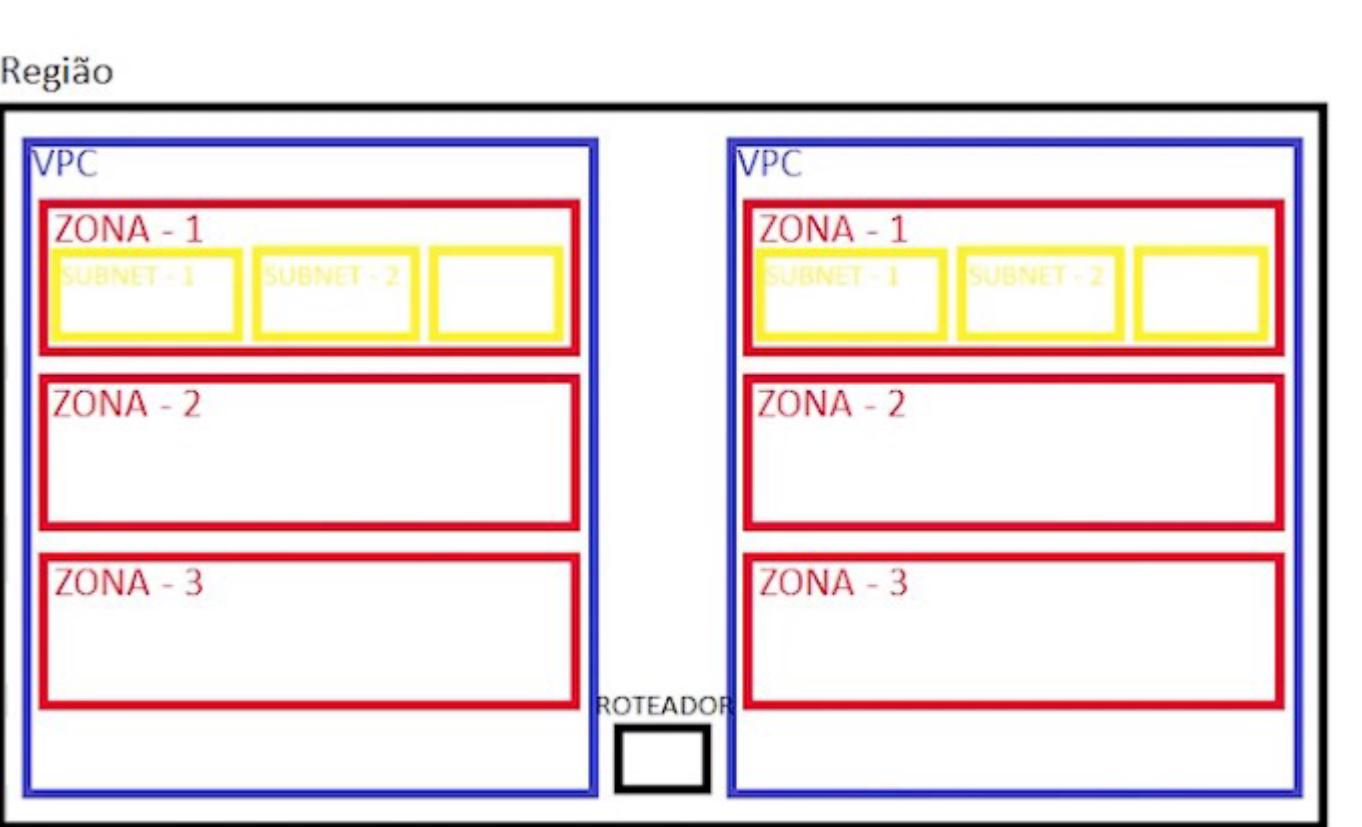
9.1. Conceito de redes

Nesta seção, vamos abordar o conceito de redes, como configurá-las e acessar a internet. Existem duas categorias principais de redes: as públicas e as privadas. As redes privadas oferecem um nível adicional de proteção em relação ao tráfego proveniente da internet. Quando o seu computador está conectado ao roteador via cabo ou Wi-Fi, é por meio dele que o tráfego para a internet é encaminhado, alcançando o gateway.

Ao estabelecer uma rede privada, adicionamos uma camada de segurança entre o roteador e o computador. Em ambientes residenciais, não há essa camada de segurança, o que torna mais fácil para hackers acessarem informações. Por isso, é importante configurar redes privadas virtuais (VPNs), conhecidas como VPCs (Virtual Private Clouds), que são redes dentro de regiões específicas, como por exemplo, "us-east-1" em provedores de serviços em nuvem.

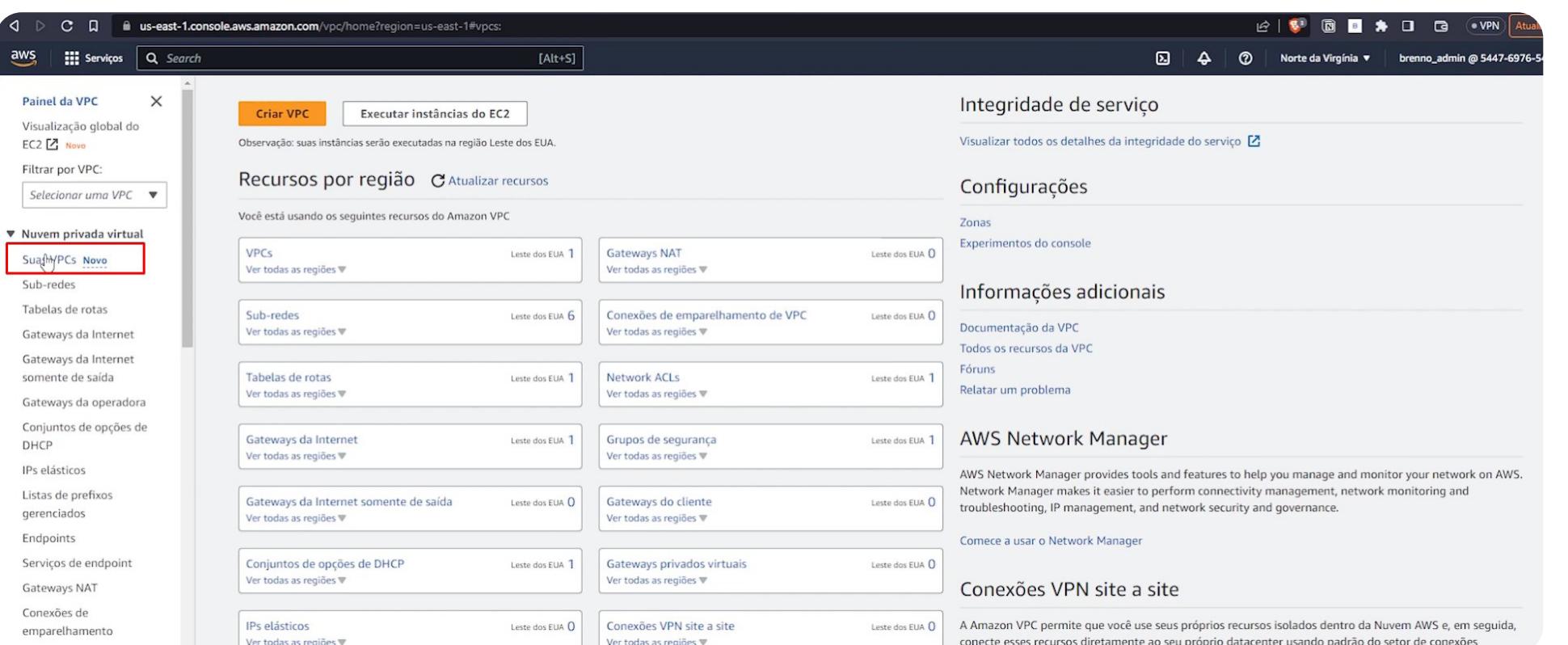
Adicionalmente, o conceito de subnet (sub-rede) refere-se a uma divisão de uma rede privada maior em redes menores e mais gerenciáveis. Essas sub-redes são úteis para organizar e controlar o tráfego de dados dentro da rede privada, oferecendo uma camada extra de segurança e permitindo uma melhor gestão dos dispositivos conectados. Conforme imagens que facilitam o entendimento.

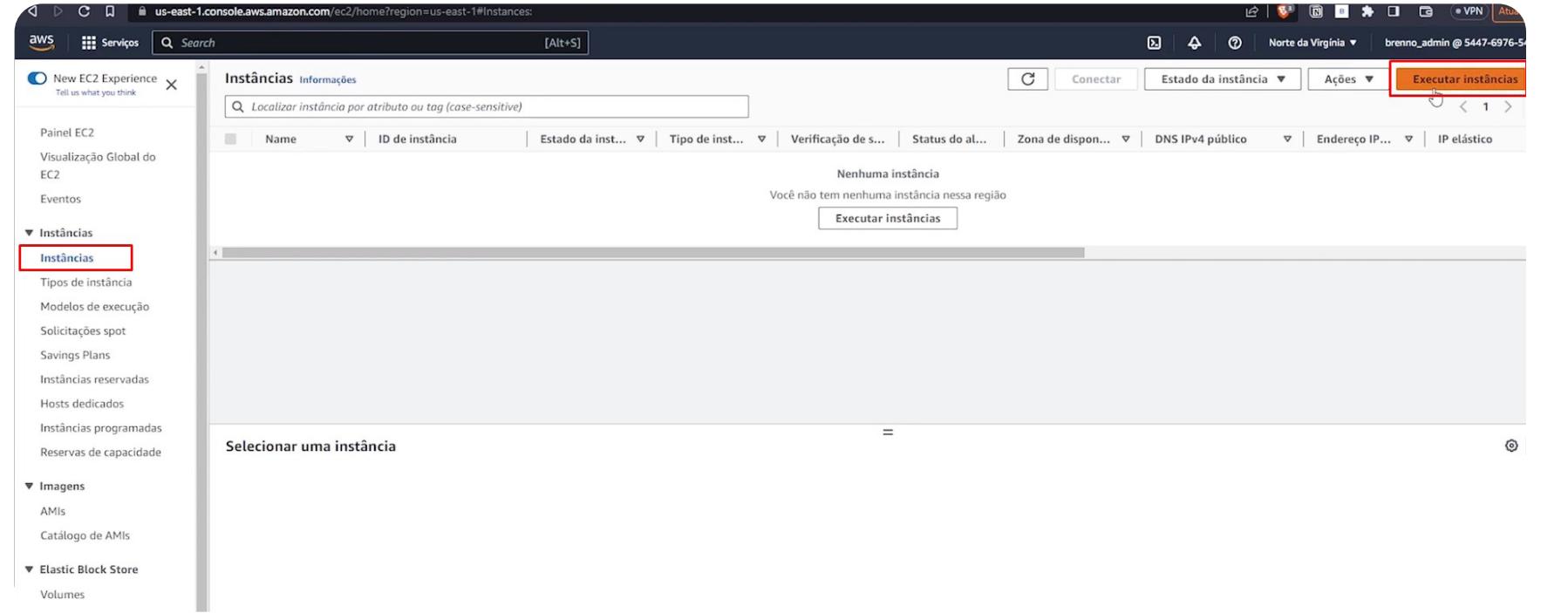




9.2. Criando VPC

Uma Virtual Private Cloud (VPC) é um serviço oferecido pela AWS, que também pode ser chamado de Virtual Private Network (VPN). Ela permite criar um ambiente de rede virtual isolado na nuvem, no qual você pode lançar recursos, como servidores, instâncias de bancos de dados e serviços, enquanto mantém controle sobre a rede.





Tag de nome, como diz, é nomear sua VPC.

Em "Bloco CIDR IPv4", vamos optar pela entrada manual, que é a forma que nós criaremos nosso IPv4.

IPv4 é apenas a quarta revisão do IP, é como se fosse uma versão específica.

"CIDR IPv4" será onde você vai criar seu IP e definir porta e conexão de rede, o 1º número refere-se à porta (neste exemplo, 10), enquanto o último refere-se à conexão conexão de rede (neste exemplo, 24).

Quanto à locação, há 2 tipos:

. Locação padrão: Funciona como uma internet banda larga, onde a operadora oferece internet numa única rede para uma região ou um bairro, e essa internet é compartilhada por várias pessoas, sendo suscetível à quedas, rede lenta e a capacidade limitada, com o aumento de pessoas.

. Locação dedicada: Neste modo, é somente uma única rede dedicada somente à você.

The screenshot shows the 'Configurações da VPC' (VPC Configuration) page. It includes sections for 'Recursos a serem criados' (Resources to be created), 'Tag de nome - opcional' (Name tag - optional), 'Bloco CIDR IPv4' (CIDR Block IPv4), 'CIDR IPv4' (CIDR IPv4), 'Bloco CIDR IPv6' (CIDR Block IPv6), 'Locação' (Location), and 'Tags'. A tag 'Varos VPC' is added. The 'Criar VPC' button at the bottom is highlighted with a red box.

9.3. Criação de sub-rede

Como na imagem ilustrada no início deste mundo 9, iremos criar algumas sub-redes, que possuem características distintas, algumas com acesso à internet, e outra sem.

The screenshot shows the 'Sub-redes' (Subnets) page with a table listing 6 subnets. The columns include 'Endereços IPv4 disponíveis' (Available IPv4 addresses), 'Zona de disponibilidade' (Availability zone), 'ID de zona de disponibili...', 'Grupo de borda de rede' (Border group), 'Tabela de rotas' (Route table), 'Network ACL', and 'Sub-rede pa...'. A new subnet entry is being added, with the 'Criar sub-rede' button highlighted with a red box.

Endereços IPv4 disponíveis	Zona de disponibilidade	ID de zona de disponibili...	Grupo de borda de rede	Tabela de rotas	Network ACL	Sub-rede pa...
4091	us-east-1e	use1-az3	us-east-1	rtb-0abcf1422e5425d1	acl-0db43d47754a0c10c	Sim
4091	us-east-1c	use1-az4	us-east-1	rtb-0abcf1422e5425d1	acl-0db43d47754a0c10c	Sim
4091	us-east-1b	use1-az2	us-east-1	rtb-0abcf1422e5425d1	acl-0db43d47754a0c10c	Sim
4091	us-east-1f	use1-az5	us-east-1	rtb-0abcf1422e5425d1	acl-0db43d47754a0c10c	Sim
4091	us-east-1d	use1-az6	us-east-1	rtb-0abcf1422e5425d1	acl-0db43d47754a0c10c	Sim
4091	us-east-1a	use1-az1	us-east-1	rtb-0abcf1422e5425d1	acl-0db43d47754a0c10c	Sim

Portanto, VPC criada.

Como pode notar, há 2 VPC, uma padrão da AWS (1^a) e outra que é referente a VPC que acabou de ser criada.

VPC > Sub-redes > Criar sub-rede

Criar sub-rede Informações

VPC

ID da VPC
Crie sub-redes nessa VPC.

Selecionar uma VPC

vpc-09e4328df55ba99d6 (padrão)
172.31.0.0/16

vpc-021c195a3b8d2aa78 (Varos VPC)
10.0.0.0/16

Selezione uma VPC primeiro para criar novas sub-redes.

Adicionar nova sub-rede

Criar sub-rede

Nas configurações de sub-rede, definiremos um nome, a zona de disponibilidade que pode ser colocada em qualquer lugar ou todas na mesma, contudo, o serviço tem que estar na mesma zona de disponibilidade que a sub-rede.

Como criaremos 3 sub-redes, em "Bloco CIDR IPv4", colocaremos o IP da VPC, com algumas mudanças.

Para a sub-rede 1: 10.0.1.0/24

Para a sub-rede 2: 10.0.2.0/24

Para a sub-rede 3: 10.0.3.0/24

Todos estes IP's, são privados, não há IP público, justamente pelo motivo de não haver conexão com a internet. Porém, por padrão, é bom ter algumas sub redes para conectar-se à internet. Ao isolar as sub-redes do mundo externo, torna-se impossível hackear seu computador.

O motivo da criação de várias sub-redes, é a distribuição do tráfego na rede privada, visando a escalabilidade e não colocar todos os recursos conectados em apenas uma única rede, aumentando assim, sua segurança.



Configurações de sub-rede
Especifique os blocos CIDR e a zona de disponibilidade para a sub-rede.

Sub-rede 1 de 1

Nome da sub-rede
Crie uma tag com a chave 'Nome' e um valor que você especificar.

O nome pode ter até 256 caracteres.

Zona de disponibilidade [Informações](#)
Escolha a zona na qual sua sub-rede residirá ou deixe que a Amazon escolha uma para você.

Bloco CIDR IPv4 [Informações](#)

Tags - opcional
Nenhuma tag associada ao recurso.

Adicionar nova tag
Você pode adicionar mais 50 tags.

Adicionar nova sub-rede

9.3.1. Conectando às sub-redes na internet

Você criou 1 sub-rede com êxito: subnet-0bdc8f4125eec1d06

Name	ID da sub-rede	Estado	VPC	CIDR IPv4	CIDR IPv6
varos - sub - c - INTERNET	subnet-0bdc8f4125eec1d06	Available	vpc-021c195a3b8d2aa78	10.0.3.0/24	-

Detalhes

VPC > Sub-redes > subnet-0bdc8f4125eec1d06 > Editar configurações de sub-rede

Editar configurações de sub-rede

Sub-rede

ID da sub-rede: Nome:

Configurações de atribuição automática de IP [Informações](#)
Habilite as configurações de atribuição automática de IP para solicitar automaticamente um endereço IPv4 ou IPv6 público para uma nova interface de rede nesta sub-rede.

Habilitar endereço IPv4 público de atribuição automática [Informações](#)

Habilitar atribuição automática de endereço IPv4 de propriedade do cliente [Informações](#)
Opção desabilitada porque nenhum grupo de propriedades do cliente foi encontrado.

9.4. Criação de roteador público

Nesta seção, será criado um roteador público para conectar-se à Internet Gateway. Como bem explicado conforme imagem no início deste mundo, não é recomendado ter apenas um roteador, é bom haver mais e configurar todos os roteadores para todas as sub-redes, tendo um roteador apenas para redes públicas e outro somente para redes privadas, isolando-as.

Como pode notar, há 2 roteadores, o 1º é o roteador padrão da AWS, e o 2º é o roteador privado que foi criado sem acesso à internet.

The screenshot shows the AWS VPC service console with the 'Route Tables' section selected. There are two route tables listed:

Name	ID da tabela de rotas	Associações explícitas de...	Associações de bor...	Princ...	VPC	ID do proprietário
-	rtb-0eabcf1422c3425d1	-	-	Sim	vpc-09e4528df55ba99d6	544769765412
-	rtb-016ec7eb2839b9506	-	-	Sim	vpc-021c195a3b8d2aa78 Varo...	544769765412

Colocaremos um nome ao nosso roteador, "Roteador Varos - Público" e adicionaremos à nossa VPC.

The screenshot shows the 'Criar tabela de rotas' (Create Route Table) wizard. The first step, 'Configurações da tabela de rotas' (Route Table Configuration), is displayed. It includes fields for:

- Nome - opcional**: A text input field containing 'my-route-table-01'.
- VPC**: A dropdown menu set to 'Selecionar uma VPC' (Select a VPC).

Below this, the 'Tags' section is shown, which is currently empty.

Vamos associar o nosso roteador público à sub-rede que haverá acesso à internet.

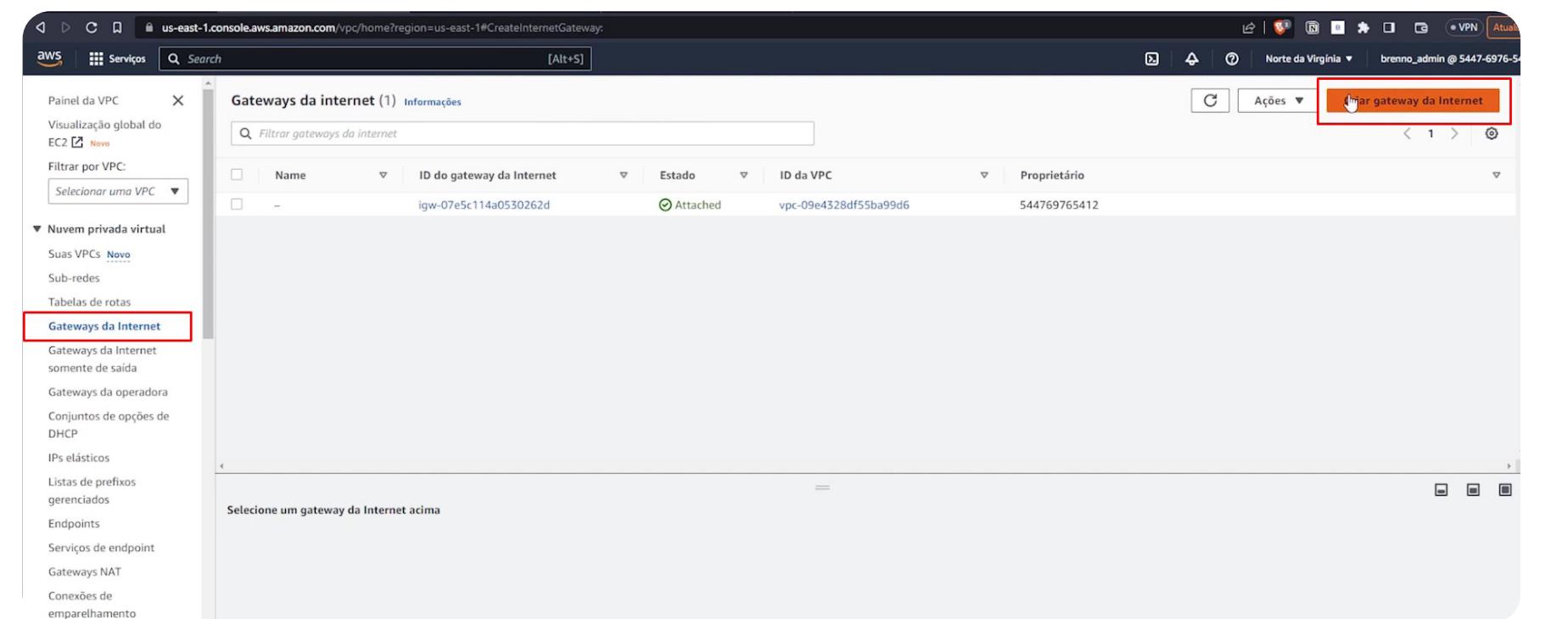
The screenshot shows the AWS VPC Route Tables page. In the main table, the row for 'Roteador VAROS - PÚBLICO' has its 'Associations de sub-rede' column set to 'Não'. A modal window titled 'rtb-05c007e936250ca05 / Roteador VAROS - PÚBLICO' is open, showing the 'Associaciones de sub-rede' tab selected. It lists three subnets: 'varos - sub - a', 'varos - sub - b', and 'varos - sub - c - INTERNET'. The 'varos - sub - c - INTERNET' checkbox is checked and highlighted with a red border. At the bottom right of the modal is a yellow 'Salvar associações' button.

Também vamos associar nosso roteador privado à sub-rede que não haverá acesso à internet.

The screenshot shows the AWS VPC Route Tables page. In the main table, the row for 'Roteador VAROS - PRIVADO' has its 'Associations de sub-rede' column set to 'Sim'. A modal window titled 'rtb-016ec7eb2839b9306 / Roteador VAROS - PRIVADO' is open, showing the 'Associaciones de sub-rede' tab selected. It lists three subnets: 'varos - sub - a', 'varos - sub - b', and 'varos - sub - c - INTERNET'. All three checkboxes are checked and highlighted with a red border. At the bottom right of the modal is a yellow 'Salvar associações' button.

9.5. Conectando Internet Gateway ao roteador público

Como pode notar, a AWS é bem intuitiva, e muito dos passos não necessitam de explicação, somente o passo a passo é necessário para o entendimento.



Criar gateway da Internet Informações

Um gateway da Internet é um roteador virtual que conecta uma VPC à Internet. Para criar um novo gateway da Internet, especifique o nome dele abaixo.

Configurações do gateway da Internet

Tag de nome
Cria uma tag com uma chave de "Nome" e um valor que você especifica.

Tags - opcional

Uma tag é um rótulo que você atribui a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional. Você pode usar tags para pesquisar e filtrar seus recursos ou rastrear seus custos da AWS.

Chave <input type="text" value="Name"/>	Valor - opcional <input type="text" value="Varos - Intern"/> Remover
<input type="button" value="Adicionar nova tag"/>	
Você pode adicionar mais 49 tags.	

[Cancelar](#) [Criar gateway da Internet](#)

Finalizando a criação do Gateway da Internet, ao retornar à página da AWS, já haverá a opção no canto superior direito, recomendando a associação à uma VPC.

9.6. Associando o roteador público a Internet Gateway

The screenshots show the following steps:

- Screenshot 1:** Shows the 'Associate a VPC' dialog for the Internet Gateway 'igw-0f5437ffe5757398f'. A red box highlights the 'Associate a VPC' button.
- Screenshot 2:** Shows the 'RouteTables' page with three route tables listed. A red box highlights the 'Roteador VAROS - PÚBLICO' route table.
- Screenshot 3:** Shows the 'Associate à VPC (igw-0f5437ffe5757398f)' dialog. A red box highlights the search bar where 'vpc-021c195a3b8d2aa78 - Varos VPC' is typed.
- Screenshot 4:** Shows the 'rtb-05c007e936250ca05 / Roteador VAROS - PÚBLICO' details page. A red box highlights the 'Edit routes' button.

Colocaremos um IP zerado, e ao lado direito, selecionaremos a opção de “Gateway de Internet”, e automaticamente a AWS irá sugerir algumas Gateway’s através do comando “igw-”, neste exemplo, só foi criado uma, selecione ela e salve as alterações.

The screenshot shows the 'Edit routes' section of the AWS VPC console. It displays a table with columns: Destino (Destination), Alvo (Target), Status (Status), and Propagado (Propagated). A single row is selected for destination 10.0.0.0/16, which is set to target 'local' (status Ativo, propagation Não). Buttons for 'Adicionar rota' (Add route), 'Cancelar' (Cancel), 'Visualização' (View), and 'Salvar alterações' (Save changes) are visible.

The screenshot shows the 'Grupos de segurança' (Security Groups) section of the AWS VPC console. On the left, a sidebar lists various VPC-related services like EC2, Sub-redes, and Gateways. The main area shows a table titled 'Grupos de segurança (2) Informações' with columns: Name, ID do grupo de segurança, Nome do grupo de..., ID da VPC, Descrição, Proprietário, and Número de regras. Two entries are listed: 'sg-031e9d6df668e917c' (default, vpc-09e4328df55ba99d6, default VPC security group, 54476) and 'sg-0980fe0524513b084' (default, vpc-021c195a3b8d2aa78, default VPC security group, 54476). A red box highlights the 'Grupos de segurança' button in the sidebar.

The screenshot shows the same 'Grupos de segurança' section as above, but with a red box highlighting the 'Criar grupo de segurança' (Create security group) button located at the top right of the main content area.

9.7. Grupos de segurança

Nesta etapa, aprenderemos como proteger sua máquina quando estiver atribuindo um IP Público e acessando a internet, promovendo uma maior segurança dos seus dados.

Cada grupo de segurança será criado conforme a necessidade da sua máquina. Neste exemplo, iremos criar um grupo de segurança padrão e te instruir a criar de modo específico.

Coloque um nome e associe à VPC criada.

The screenshot shows the 'Criar grupo de segurança' (Create Security Group) page. In the 'Nome do grupo de segurança' field, 'SG - Varos' is entered. Under 'Descrição', 'Permite acesso SSH aos desenvolvedores' is selected. In the 'VPC' dropdown, 'vpc-09e4328df55ba99d6' is chosen. A note at the bottom states: 'Este grupo de segurança não tem regras de entrada.' (This security group has no incoming rules.)

Em regras de saída, por padrão, o grupo de segurança vem com "Todo o tráfego" para o IP "0.0.0.0/00" que é do Gateway da Internet, e isso é péssimo para a sua segurança. Portanto, selecione o mais adequado para a sua máquina. Por exemplo, se houver somente conexões com banco de dados, poderá selecionar a opção do MySQL, ou se for somente máquinas se comunicando como um AnyDesk, pode selecionar o tipo de "SSH". E para os casos que haverá o acesso à internet somente, selecione o tipo de regra de saída "HTTP".

Como explicado no início deste subcapítulo, manteremos com "todo o tráfego", mas evite e sempre escolha conforme sua necessidade.

Já na outra etapa, em "Destino", ainda dentro das "Regras de saída", podemos selecionar somente para o nosso grupo de segurança, ou outras opções a seu critério.

The screenshot shows the 'Regras de saída' (Output Rules) section. The 'Tipo' dropdown is set to 'SSH'. The 'Protocolo' dropdown is set to 'TCP'. The 'Intervalo de portas' dropdown is set to '22'. The 'Destino' dropdown shows 'default | sg-0980fe0524513b084'. A red box highlights the 'Destino' dropdown. To the right, a sidebar lists CIDR blocks: '0.0.0.0/0', '0.0.0.0/8', '0.0.0.0/16', '0.0.0.0/24', '0.0.0.0/32', '::/0', '::/16', '::/32', '::/48', '::/64', and 'Grupos de segurança' with 'default | sg-0980fe0524513b084' selected. A red box highlights the 'Destino' dropdown in the sidebar.

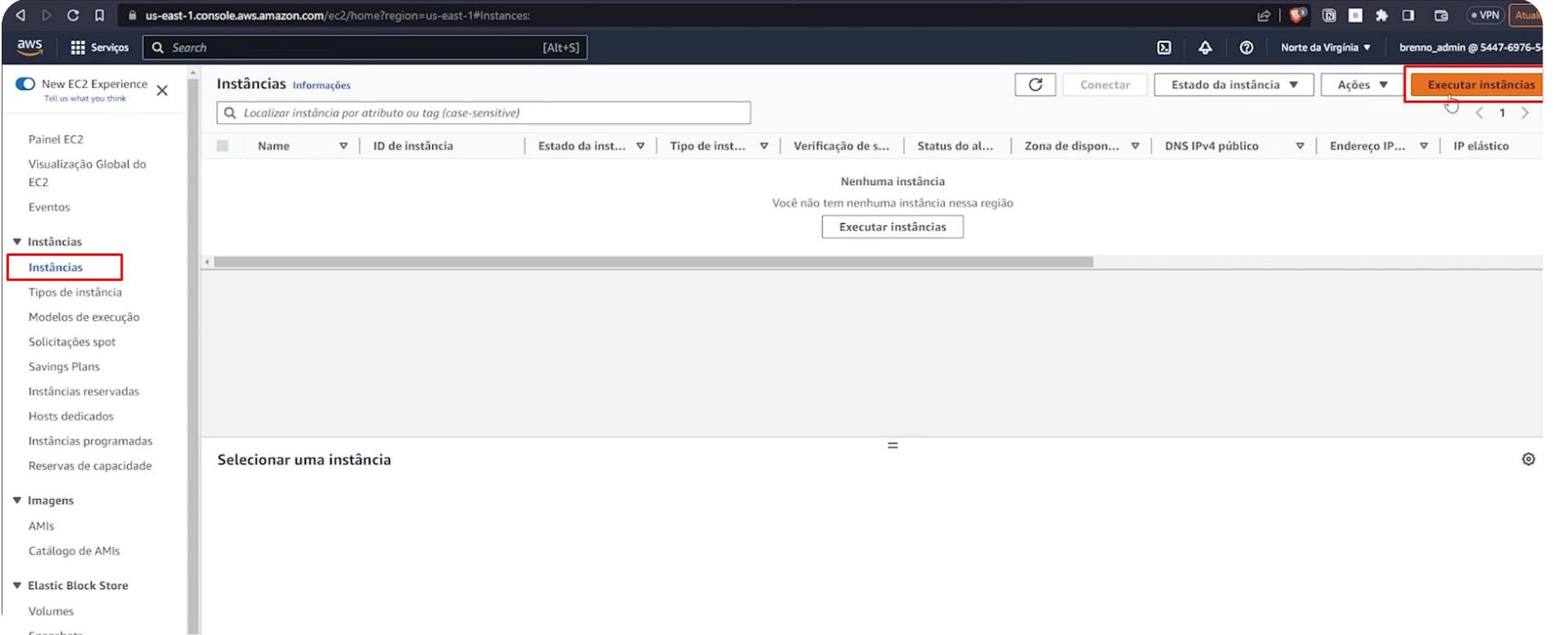
Portanto, configuramos nossa rede e adicionamos algumas camadas de proteção.

Mundo 10

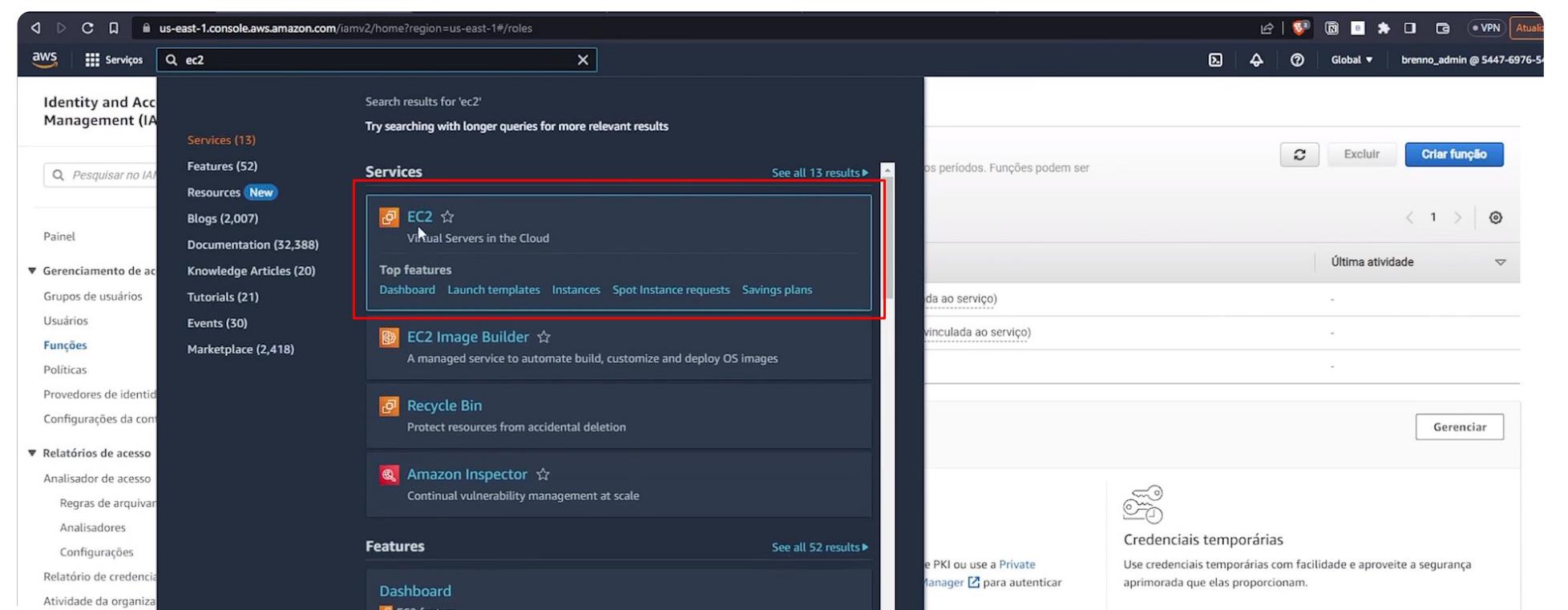
Neste mundo, aprenderemos sobre como criar uma máquina virtual e alugar computação em nuvem para rodar os códigos.

10.1. Criando uma EC2

No mundo 2, foi ensinado sobre o que é uma EC2, mas lembrando: "Serviço de máquinas virtuais (VMs) que permite criar e gerenciar servidores na nuvem. É como se fosse um computador normal, em que você escolhe a quantidade de RAM, armazenamento, CPU e etc. Adequado para hospedagem de sites, executar sistemas e rotinas pesadas, realizar análise e também rodar modelos de investimento."



Colocaremos um nome para nossa EC2, e logo abaixo, selecionamos o sistema operacional. Caso queira procurar algum outro, ou algum em específico, vá em "Procurar mais AMIs", existem mais de 500 sistemas disponíveis na AWS.



Como podemos notar, após a escolha do sistema Linux Ubuntu, ele está qualificado para o nível gratuito, dentro do nosso Free-Tier.

A configuração “Tipo de Instância” é a configuração do computador que será alugada. Caso a máquina, após gerar a instância e rodar o código, simplesmente desligue sem gerar log ou qualquer tipo de erro, é pelo motivo da máquina não aguentar e ser fraca, sendo necessário um computador mais potente.

"Par de Chaves" é o seu login na máquina, seja para mexer, subir código, etc.

The screenshot shows the AWS Lambda console configuration page. In the 'Type de instância' section, a dropdown menu is open for 't2.micro', showing its details: Qualificado para o nível gratuito, Família: t2, 1 vCPU, 1 GiB Memória, Geração atual: true, and various price definitions for Windows, SUSE, RHEL, and Linux. Below this, there are buttons for 'Todas as gerações' (All generations) and 'Comparar tipos de instância' (Compare instance types). In the 'Par de chaves (login)' section, it says you can use a key pair for secure connection. A dropdown menu is open, showing 'Selecionar' (Select) and 'Criar novo par de chaves' (Create new key pair), with the latter being the selected option.

Ao criar o par de chaves, dê um nome, como tudo na AWS. Posteriormente, mantenha o tipo de chave como RSA, e se você aprendeu tudo no GitHub, essa parte é bem fácil. RSA é o tipo de criptografia utilizada, sendo a mais utilizada no mundo entre 2 computadores. No GitHub configuramos uma chave RSA com o Git Bash, para conectarmos no GitHub através de comandos como "git push", "git pull" e etc. Por fim, não esqueça de salvar o seu par de chaves.

The screenshot shows the 'Criar par de chaves' (Create Key Pair) dialog box. It asks for a name ('Nome do par de chaves') which is set to 'Curso'. A warning message states that the name cannot start or end with spaces. It also specifies that the name can have up to 255 ASCII characters and must not contain spaces. The 'Tipo de par de chaves' (Type of key pair) section shows two options: 'RSA' (selected) and 'ED25519'. 'RSA' is described as a public and private key pair encrypted with RSA. The 'Formato de arquivo de chave privada' (Private key file format) section shows two options: '.pem' (selected) and '.ppk'. '.pem' is for OpenSSH use, and '.ppk' is for PuTTY use. A warning message at the bottom advises saving the private key in a safe location and notes that it will be needed later for connecting to the instance. At the bottom right are 'Cancelar' (Cancel) and 'Criar par de chaves' (Create key pair) buttons.

Continuando, editamos a configuração da rede para utilizar a nossa rede e sub-rede que criamos.

Configurações de rede

Rede: vpc-09e4328af55ba99d6

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

Atribuir IP público automaticamente: Informações

Habilitar

Firewall (grupos de segurança): Criaremos um novo grupo de segurança chamado "launch-wizard-1" com as seguintes regras:

- Criar grupo de segurança
- Selecionar grupo de segurança existente

Criaremos um novo grupo de segurança chamado "launch-wizard-1" com as seguintes regras:

- Permitir tráfego SSH de Qualquer lugar CIDR: 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.

Além de habilitar o IP Público, é necessário atribuir a um grupo de segurança existente, aqueles que criamos no mundo 9.

Configurações de rede

VPC - obrigatório: vpc-021c195a3b8d2aa78 (Varos VPC) CIDR: 10.0.0.0/16

Sub-rede: varos - sub - a

Criar nova sub-rede

subnet-00d7a3fa04cc7f253: varos - sub - a
VPC: vpc-021c195a3b8d2aa78 Proprietário: 544769765412 Zona de disponibilidade: us-east-1a Endereços IP disponíveis: 251 CIDR: 10.0.1.0/24

subnet-00d7a3fa04cc7f253: varos - sub - a
VPC: vpc-021c195a3b8d2aa78 Proprietário: 544769765412 Zona de disponibilidade: us-east-1a Endereços IP disponíveis: 251 CIDR: 10.0.1.0/24

subnet-06c79e6a59bbff39f: varos - sub - b
VPC: vpc-021c195a3b8d2aa78 Proprietário: 544769765412 Zona de disponibilidade: us-east-1b Endereços IP disponíveis: 251 CIDR: 10.0.2.0/24

subnet-0bdc8f4125eec1d06: varos - sub - c - INTERNET
VPC: vpc-021c195a3b8d2aa78 Proprietário: 544769765412 Zona de disponibilidade: us-east-1c Endereços IP disponíveis: 251 CIDR: 10.0.3.0/24

Nome do grupo de segurança: launch-wizard-1

Esse grupo de segurança será adicionado a todas as interfaces de rede. Não é possível editar o nome após a criação do grupo de segurança. O comprimento máximo é de 255 caracteres. Os caracteres válidos são: a-z, A-Z, 0-9, espaços e _-:/()#,@[]+=;&{}!\$*

Descrição - obrigatório: launch-wizard-1 created 2023-08-01T13:35:26.156Z

Regras do grupo de segurança de entrada

Regra de grupo de segurança 1: (TCP, 22, 0.0.0.0/0)

Remover

Quanto à configuração de armazenamento, mantenha o padrão e execute a instância.

The screenshot shows the 'Configurar armazenamento' (Configure Storage) step of the EC2 instance creation wizard. It displays a table for adding volumes:

Volumes	Tamanho (GiB)	Tipo	Ações
1x	8	gp2	Volume raiz (Não criptografado)

Below the table, there's a note about free tier usage and a link to add new volumes. At the bottom, there are 'Cancelar' (Cancel), 'Executar instância' (Run Instance) in a red box, and 'Revisar comandos' (Review Commands).

Subimos nossa primeira máquina virtual na AWS, mas se tentarmos conectar ao computador, haverá um erro, pois como padrão na AWS, tudo é bloqueado e precisa haver permissões. Portanto, concedemos a permissão ao EC2 para conectar a internet. Portanto, retorne à VPC, em "Grupo de segurança", como instruído no mundo 9, e selecione o grupo de segurança que criamos.

The screenshot shows the 'Grupos de segurança (1/3)' (Security Groups) page. A table lists three security groups:

Name	ID do grupo de seg...	Nome do grupo de ...	ID da VPC	Descrição	Proprietário	Número de regras ...	Número de regras ...
sg-03dcbd2977efc14bc	sg-03dcbd2977efc14bc	SG - Varos	vpc-021c195a3b8d2aa78	Teste codigopy	544769765412	0 Entradas de permissão	1 Entrada de permissão
sg-031e6d6df668e917c	sg-031e6d6df668e917c	default	vpc-09e4328df55ba99d6	default VPC security gr...	544769765412	1 Entrada de permissão	1 Entrada de permissão
sg-0980fe0524513b084	sg-0980fe0524513b084	default	vpc-021c195a3b8d2aa78	default VPC security gr...	544769765412	1 Entrada de permissão	1 Entrada de permissão

The 'SG - Varos' group is highlighted with a red box. Below the table, there are tabs for 'Detalhes', 'Regras de entrada', 'Regras de saída', and 'Tags'. The 'Regras de saída' tab is selected.

Antes de nos conectarmos, é preciso inserir uma regra de entrada que não existe, há somente a porta de saída. A única configuração que realizamos na configuração do grupo de segurança foi a regra de saída que colocamos para “todo o tráfego”. Logo, se não há regra de entrada, não há possibilidade de entrar na máquina.

Name	ID da regra do grupo de segurança	Versão do IP	Tipo	Protocolo	Intervalo de portas
sgr-08434398e84ddcbff	IPv4	Todo o tráfego	Tudo	Tudo	

Em regras de entrada, no lado direito, clique em “editar regras de entrada”.

Name	ID da regra do grupo de segurança	Versão do IP	Tipo	Protocolo	Intervalo de portas

Nenhuma regra de grupo de segurança encontrada

Coloque o seu IP mesmo, e salve as alterações. Em caso de persistência do erro, modifique e coloque “Qualquer local IPv4”.

ID da regra do grupo de segurança	Tipo	Protocolo	Intervalo de portas	Origem	Descrição - opcional
-	SSH	TCP	22	Meu IP	

Retorne ao EC2, e nos conectamos à nossa máquina.

Name	ID da instância	Estado da instância	Tipo de instância	Verificação de segurança	Status do alerta	Zona de disponibilidade	DNS IPv4 público	Endereço IP privado	IP elástico
EC2 Teste	i-0befa60b373636eb6	Executando	t2.micro	-	Sem alerta	+ us-east-1c	-	34.228.54.237	-

EC2 > Instâncias > i-0befa60b373636eb6 > Conectar-se à instância

Conectar-se à instância Informações

Conecte-se à sua instância i-0befa60b373636eb6 (EC2 Teste) usando qualquer uma destas opções

Conexão de instância do EC2 Gerenciador de sessões Cliente SSH Console de série do EC2

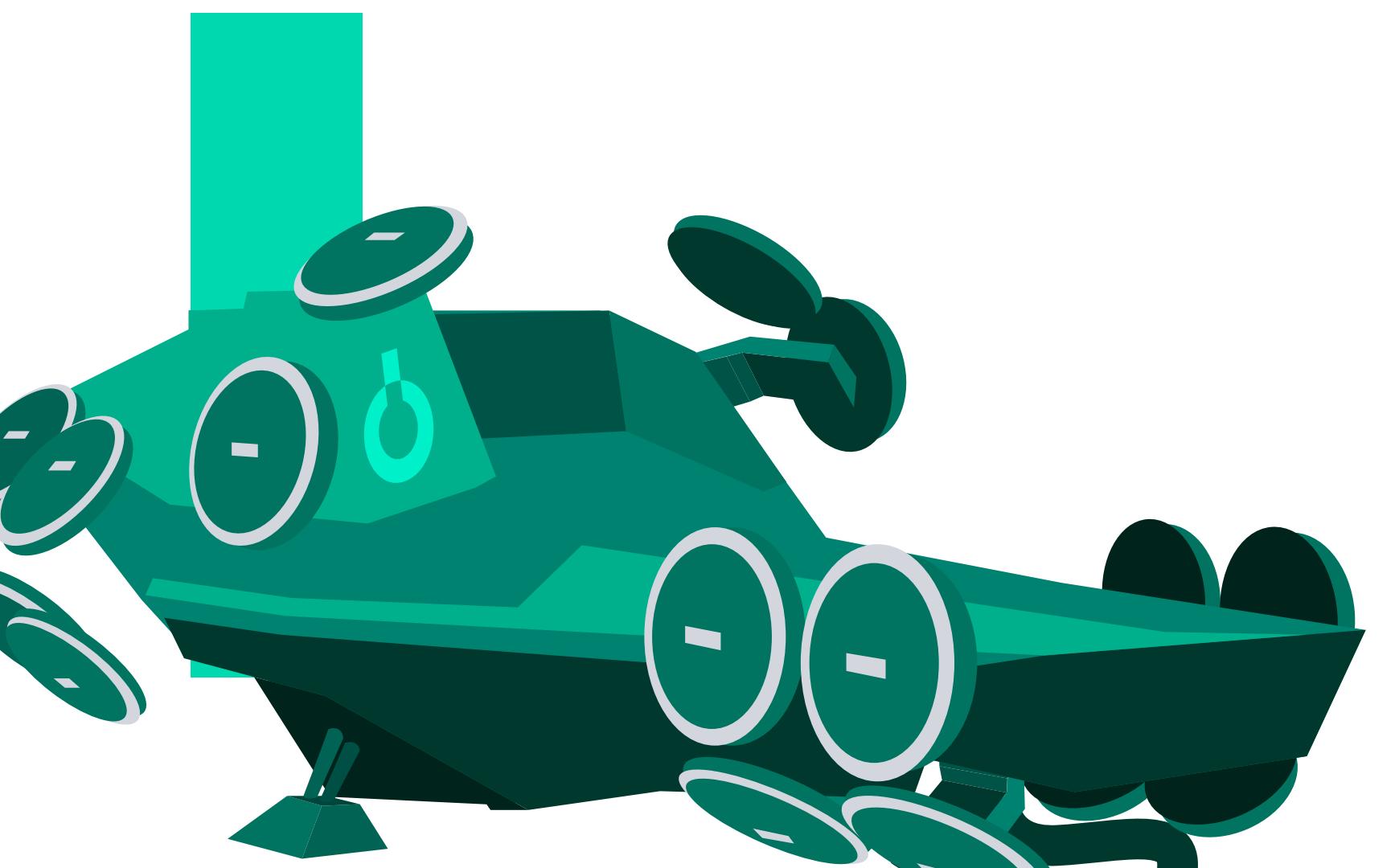
ID de instância
 i-0befa60b373636eb6 (EC2 Teste)

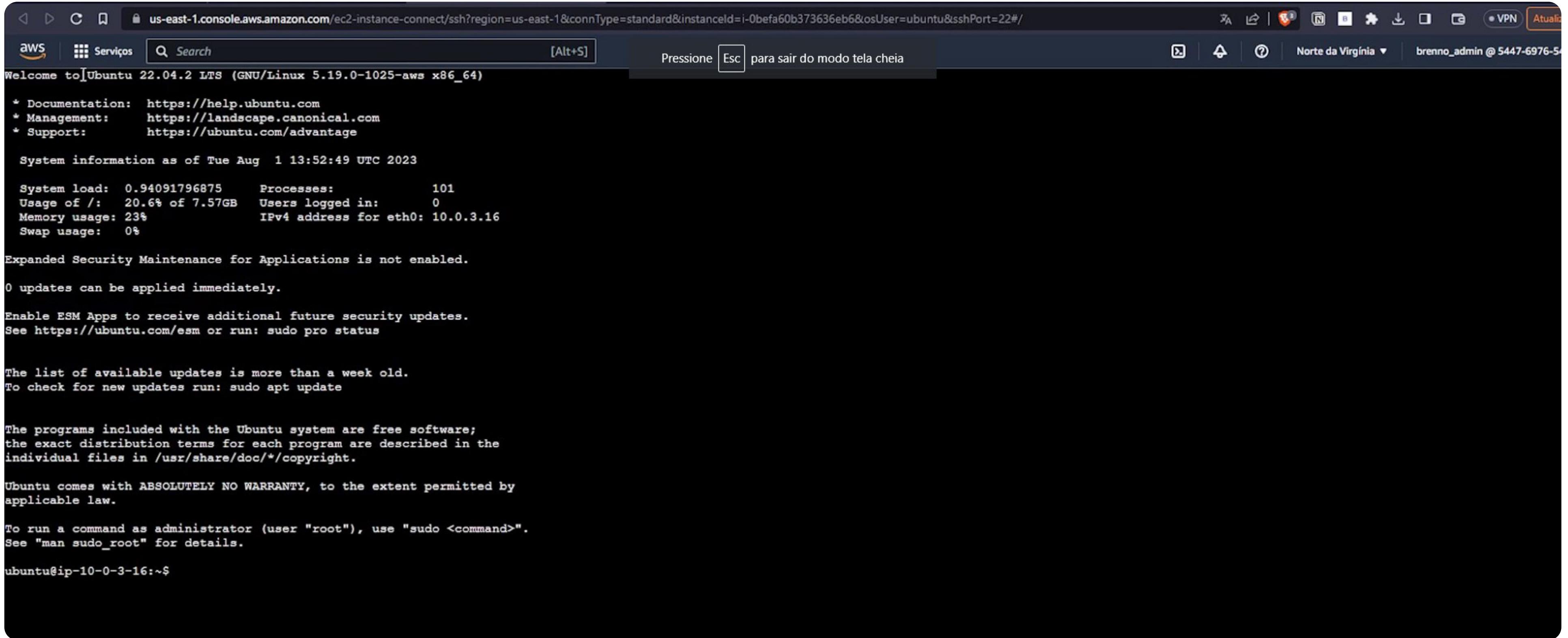
Tipo de conexão
 Conectar-se usando o EC2 Instance Connect
Conecte-se usando o cliente baseado em navegador do EC2 Instance Connect, com um endereço IPv4 público.
 Conectar-se usando o endpoint do EC2 Instance Connect
Conecte-se usando o cliente baseado em navegador do EC2 Instance Connect, com um endereço IPv4 privado e um endpoint da VPC.

Endereço IP público
 34.228.54.237

Nome do usuário
Insira o nome de usuário definido na AMI usada para iniciar a instância. Se você não definiu um nome de usuário personalizado, use o nome de usuário padrão, ubuntu.

Observação: na maioria dos casos, o nome de usuário padrão, ubuntu, está correto. No entanto, leia as instruções de uso da AMI para verificar se o proprietário da AMI alterou o nome de usuário da AMI padrão.



A screenshot of a web-based terminal session from AWS. The URL in the address bar is "us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0befa60b373636eb6&osUser=ubuntu&sshPort=22#/" . The title bar shows "AWS | Serviços | Search [Alt+S]" and "Pressione Esc para sair do modo tela cheia". The main content is a terminal window displaying the following text:

```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

System information as of Tue Aug  1 13:52:49 UTC 2023

System load: 0.94091796875    Processes:          101
Usage of /: 20.6% of 7.57GB   Users logged in: 0
Memory usage: 23%           IPv4 address for eth0: 10.0.3.16
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-3-16:~$
```

Conexão estabelecida com sucesso, iniciaremos nossos projetos. Porém, não esqueça de encerrar a instância após o uso.

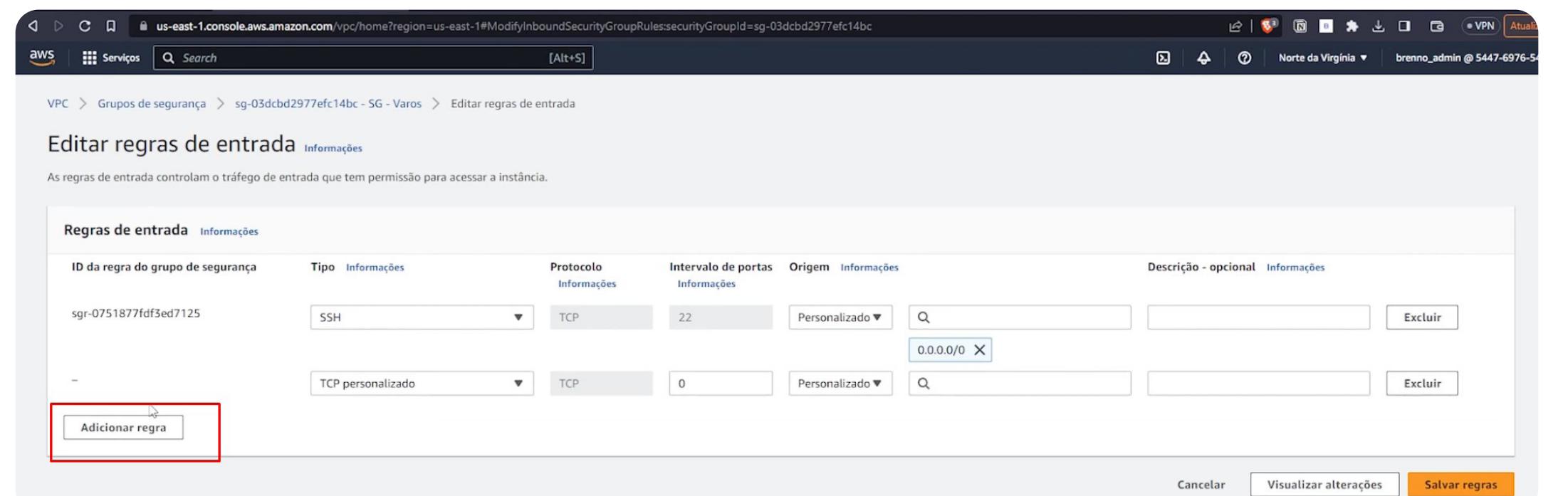
Screenshot of the AWS EC2 Instances page. The instance 'EC2 Teste' (i-0befa60b373636eb6) is listed. The 'Actions' menu is open, and the 'Encerrar instância' (Shutdown) option is highlighted with a red box.

Screenshot of the 'Encerrar instância?' (Shutdown instance?) confirmation dialog. It contains a warning message about root volume deletion and two buttons: 'Cancelar' (Cancel) and 'Encerrar' (Shutdown), with the 'Encerrar' button highlighted with a red box.

Projeto 1: Dashboard Online

Criaremos um EC2 somente para este projeto. Vamos nomear de EC2 Dashboard Online, com o sistema operacional Ubuntu Linux, utilizando o mesmo par de chaves e configurações de rede que criamos no mundo 10. Será mostrado somente as etapas que não foram ensinadas até este momento, em caso de dúvida, basta retornar aos mundos anteriores.

Como este projeto é sobre um dashboard online, utilizando Internet Gateway, obviamente poderá ser acessado de qualquer localidade. Portanto, vá em **VPC → Grupos de Segurança → Regras de Entrada**. Será modificado as regras de entrada, pois é preciso a conexão com a internet e entre máquinas, ou seja, SSH e HTTP.



Portas TCP são identificadores numéricos usados para especificar diferentes tipos de tráfego de rede. Elas são usadas para direcionar o tráfego de acordo com os protocolos de comunicação e os tipos de serviços que estão sendo acessados. Por exemplo:

A porta 80 é comumente usada para o protocolo HTTP, que é utilizado para acessar páginas da web. A porta 443 é utilizada pelo protocolo HTTPS, fornecendo uma conexão segura para páginas da web através de SSL/TLS. A porta 22 é frequentemente utilizada para conexões SSH, permitindo acesso seguro a servidores.

Quando você configura regras de segurança em um grupo de segurança na AWS para permitir ou bloquear o tráfego, você especifica as portas TCP que deseja abrir para o tráfego de entrada ou saída. Por exemplo, se você estiver executando um servidor web em uma instância na AWS, precisará abrir a porta 80 (HTTP) ou a porta 443 (HTTPS) para permitir que o tráfego web chegue a essa instância.

TCP Personalizado trata-se de acesso para a mesma rede. Exemplo: O Dashboard pode ser acessado somente para o seu escritório que está conectado na mesma rede (internet/wi-fi).

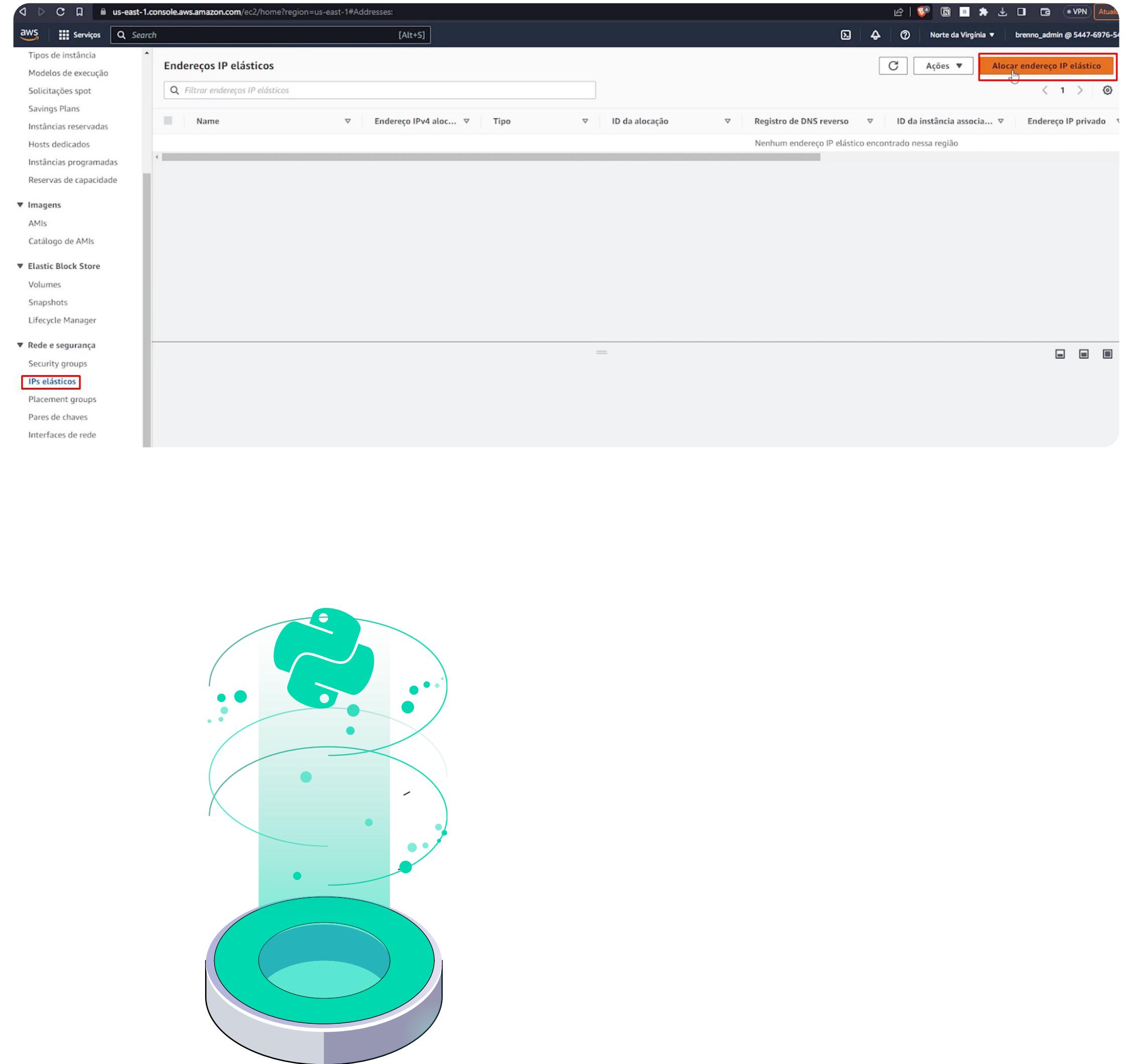
ID da regra do grupo de segurança	Tipo	Protocolo	Intervalo de portas	Origem	Descrição - opcional
sgr-0751877fdf3ed7125	SSH	TCP	22	Personalizado	0.0.0.0/0
-	HTTP	TCP	80	Qualquer l...	0.0.0.0/0
-	HTTPS	TCP	443	Qualquer l...	0.0.0.0/0
-	TCP personalizado	TCP	8080	Qualquer l...	0.0.0.0/0
					Adicionar regra

Após as configurações, pode retornar ao EC2, mas é necessário realizar outra alteração em relação ao IP público.

Na AWS, por padrão, toda vez que desligamos e ligamos uma máquina, a Amazon atribui um novo IP público para o computador, ou seja, toda vez esse IP é trocado. Contudo, para esse dashboard, é imprescindível que mantenha somente um IP, isso é o que chamamos de IP's Elásticos, pois essa será a forma de acessar o dashboard online, caso contrário, nunca saberemos qual é o IP de acesso.

Para esclarecimento, segue um exemplo: toda vez que você vai entrar em algum site, como o da Globo, você digita "www.globo.com". Essa foi a maneira que aprendemos desde a infância. Porém, essa url, assim como qualquer uma, está associada a um IP, e se você tentar acessar pelo IP Público "186.192.90.12", também terá sucesso, faça o teste em casa.

Portanto, definiremos um IP público único para nosso dashboard, sem mudanças quando desligamos a máquina.



This screenshot shows the 'Alocar endereço IP elástico' configuration page. It includes sections for 'Configurações de endereço IP elástico' (with a search bar for 'us-east-1'), 'Grupo de Borda de Rede' (with a search bar for 'us-east-1'), 'Conjunto de endereços IPv4 públicos' (with three options: 'Conjunto de endereços IPv4 da Amazon' (selected), 'Endereço IPv4 público que você leva para sua conta da AWS' (disabled), and 'Grupo com os endereços IPv4 pertencentes ao cliente' (disabled)), 'Endereços IP estáticos globais' (with a note about AWS Global Accelerator), and 'Tags opcional' (with a note about tags). At the bottom right, there are 'Cancelar' and 'Alocar' buttons, with 'Alocar' highlighted with a red box.

Após, será gerado um IP Único, renomeie, neste caso colocamos "Dashboard público", e depois faça associação ao EC2 Dashboard Online.

The screenshot shows the AWS EC2 console with a green success message: "Endereço IP elástico alocado com sucesso. Endereço IP elástico 44.209.250.166". Below it, the "Endereços IP elásticos (1/1)" table lists one entry: "Dashboard público" with IP "44.209.250.166". A context menu is open over this entry, with the "Associar endereço IP elástico" option highlighted.

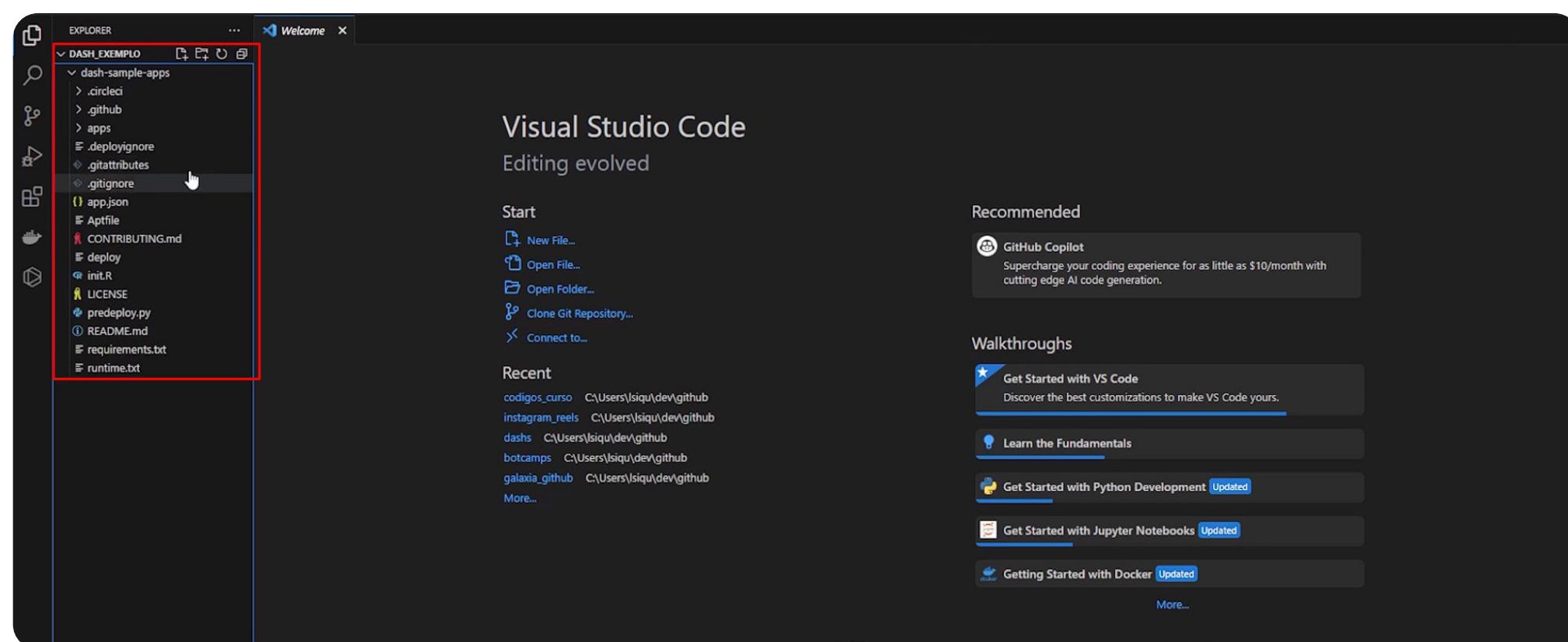
The screenshot shows the "Associate elastic IP address" dialog. It displays the elastic IP address "44.209.250.166" and asks to select a resource type: "Instância" (selected) or "Interface de rede". A warning message states: "Se você associar um endereço IP elástico a uma instância que já tem um endereço IP elástico associado, o endereço existente será desassociado, mas ainda estará alocado à sua conta. Saiba mais". Below, it says: "If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address." The "Instância" search field contains "i-0a9cf9b3465d81e7e", which is also highlighted with a red box. The "Cancelar" and "Associar" buttons are at the bottom, with "Associar" also highlighted with a red box.

O dashboard que iremos utilizar é um pronto da própria biblioteca de dash. Neste caso, iremos apenas clonar um repositório do GitHub, no caso, clonar um dashboard da própria biblioteca de dash do python, pronto para subir no nosso dashboard numa URL padrão.

<https://github.com/plotly/dash-sample-apps>

Como aprendido na galáxia de GitHub, em seu computador, na pasta separada para o GitHub, crie uma pasta para o dashboard. Depois abra a pasta no VSCode, crie um terminal, vá ao Git Bash, e clone o dashboard selecionado com o comando:

git clone https://github.com/plotly/dash-sample-apps.git



Agora, dentro desta pasta, iremos iniciar um repositório seu, fazendo novamente um "Open Folder" na pasta, abrindo um novo terminal do Git Bash, e dando o comando:

git init

Siga esses passos para entrar no código e modificar a última linha do código:

```

EXPLORER          app.py
DASH_EXEMPLO      apps > app.py >-
> .circleci      score_selected_index = selected_index
> .github         department_score_figure = create_table_figure(
> .github          department,
> .github          filtered_df,
> .github          "Care Score",
> .github          score_xrange,
> .github          score_selected_index,
> .github          )
> .github          figure_list.append(department_score_figure)
> .github          # Put figures in table
> .github          table = generate_patient_table(
> .github          | figure_list, departments, wait_time_xrange, score_xrange
> .github          )
> .github          return table
> .github          739 # Run the server
> .github          740 if __name__ == "__main__":
> .github          741     app.run_server(debug=True)
> .github          742
> assets
> data
> img
> dash-clinical-analytics
> dash-clinical-analytics
> assets
> data
> img
> app.py
> Profile
> README.md
> requirements.txt
> dash-covid-xray
> dash-cuml-umap
> dash-cytoscape
> dash-cytoscape-editor
> dash-cytoscape-ldi
> dash-cytoscape-phylogeny
> dash-daq-tracer
> dash-daq-satellite-dashboard
> dash-daq-tektronix350
    
```

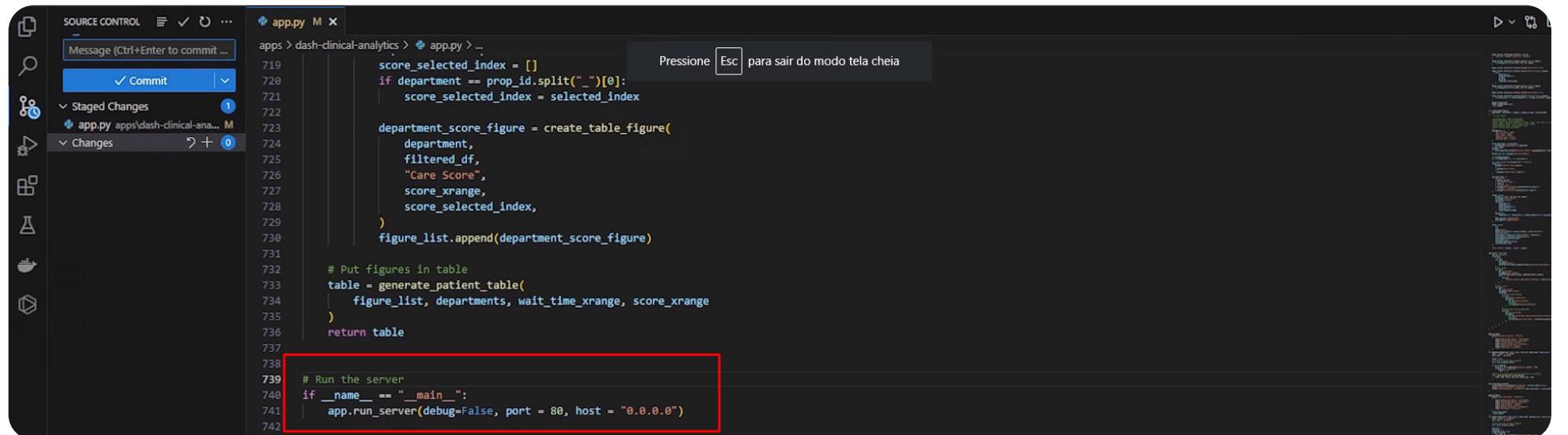
Modifique o código, de:

```
app.run_server(debug = True)
```

para:

```
app.run_server(debug = False, port = 80, host = "0.0.0.0")
```

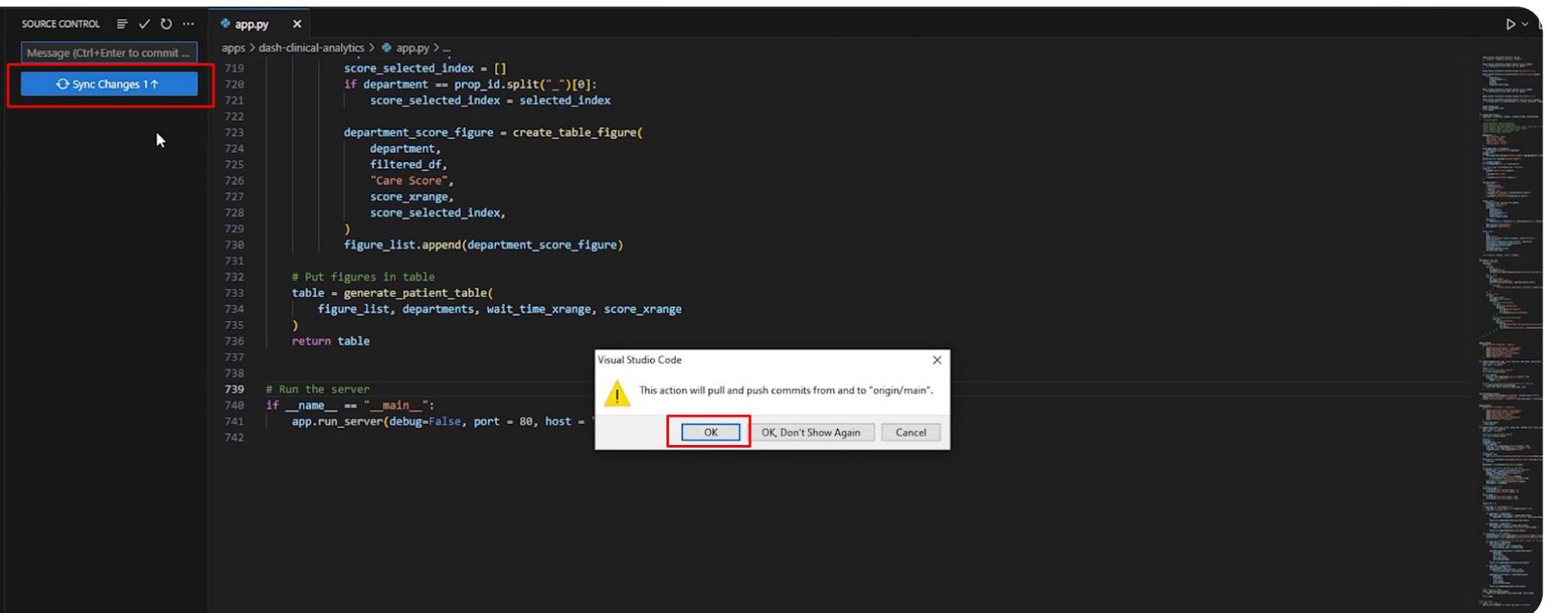
Vamos somente postar, na porta 80, que foi a porta que colocamos como uma das regras de entrada do nosso grupo de segurança que criamos lá no início.



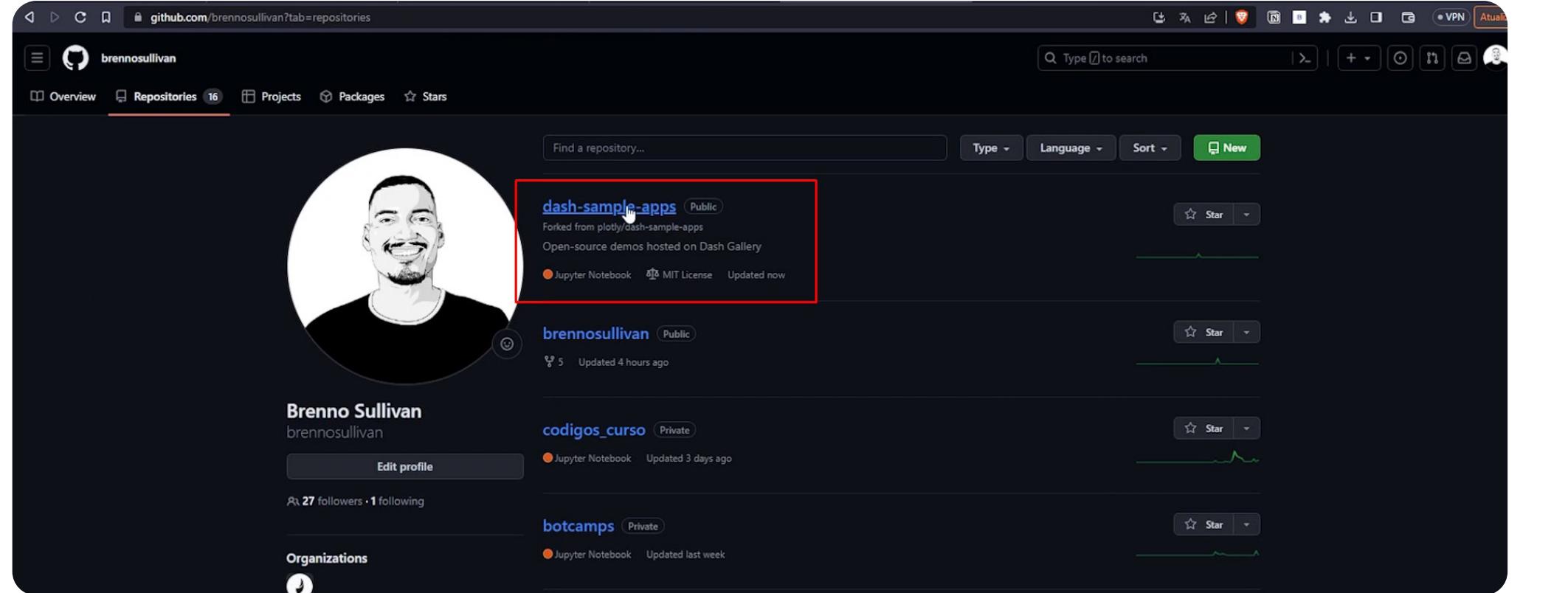
Para finalizar, como sempre, dê um commit:

```
git add .
```

```
git commit -m "alterando pro EC2"
```



E assim, publicaremos no seu próprio GitHub.



Agora é hora de upar o Dashboard no EC2 que foi criado. Executando a instância do EC2 Dashboard Online, ao abrir o prompt de comando:

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0befa60b373636eb6&osUser=ubuntu&sshPort=22/
[Alt+S] Pressione [Esc] para sair do modo tela cheia
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Tue Aug 1 13:52:49 UTC 2023

System load: 0.34031796875 Processes: 101
Usage of /: 20.6% of 7.57GB Users logged in: 0
Memory usage: 23% IPv4 address for eth0: 10.0.3.16
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-3-16:~$
```

Toda vez que o Linux for inicializado, é importante que digite esse código, para dar update em todos os pacotes necessários.

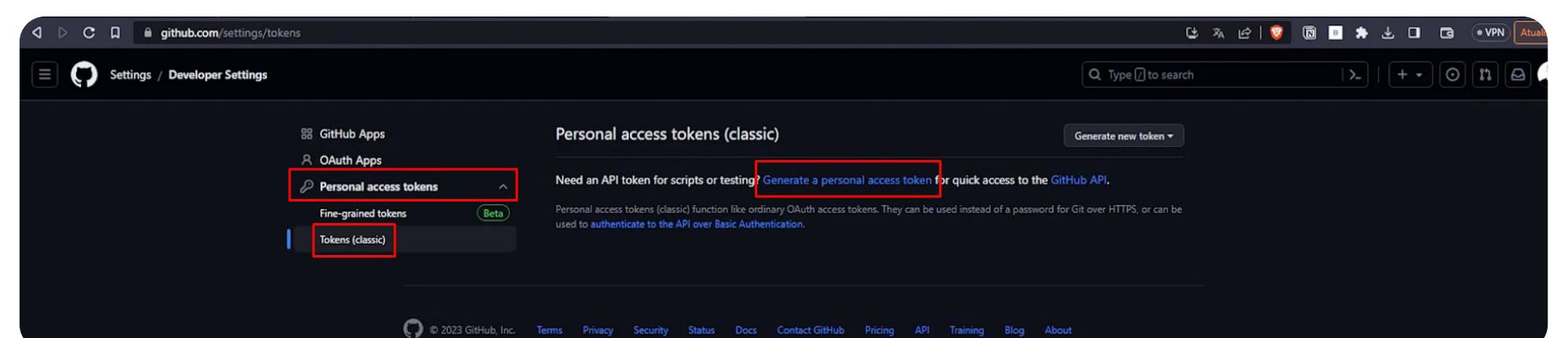
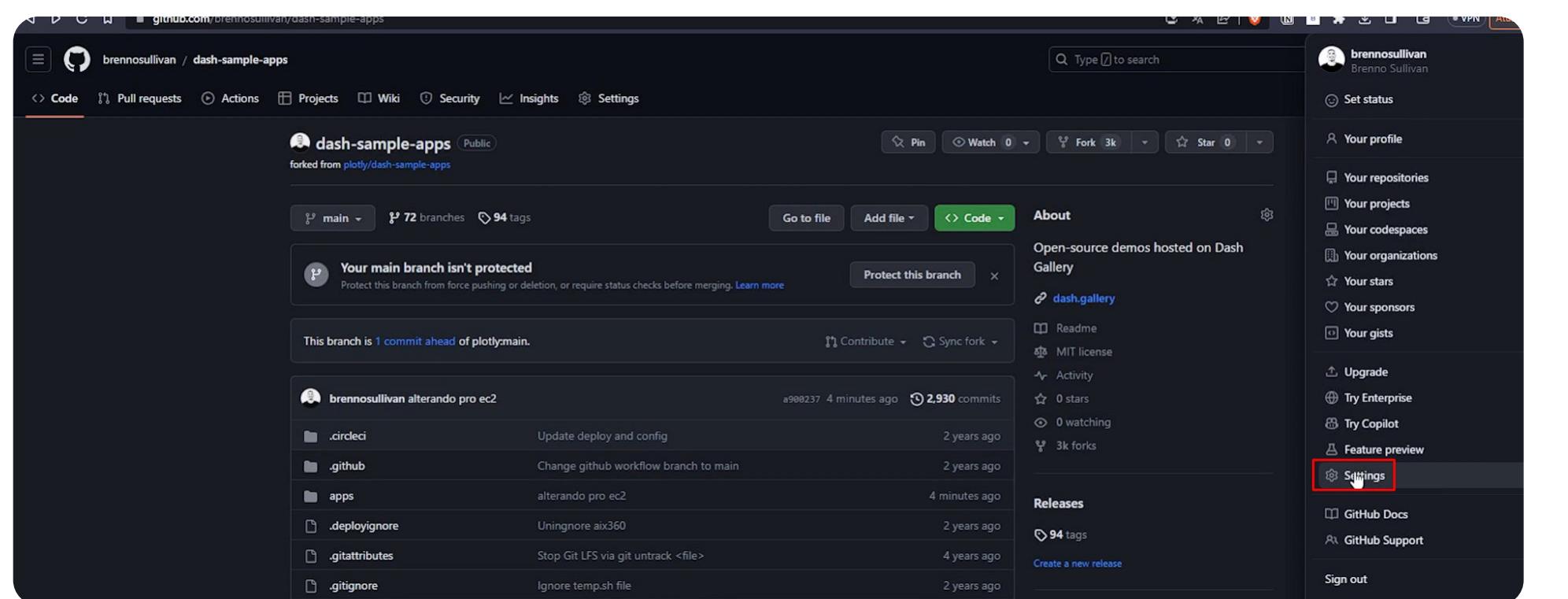
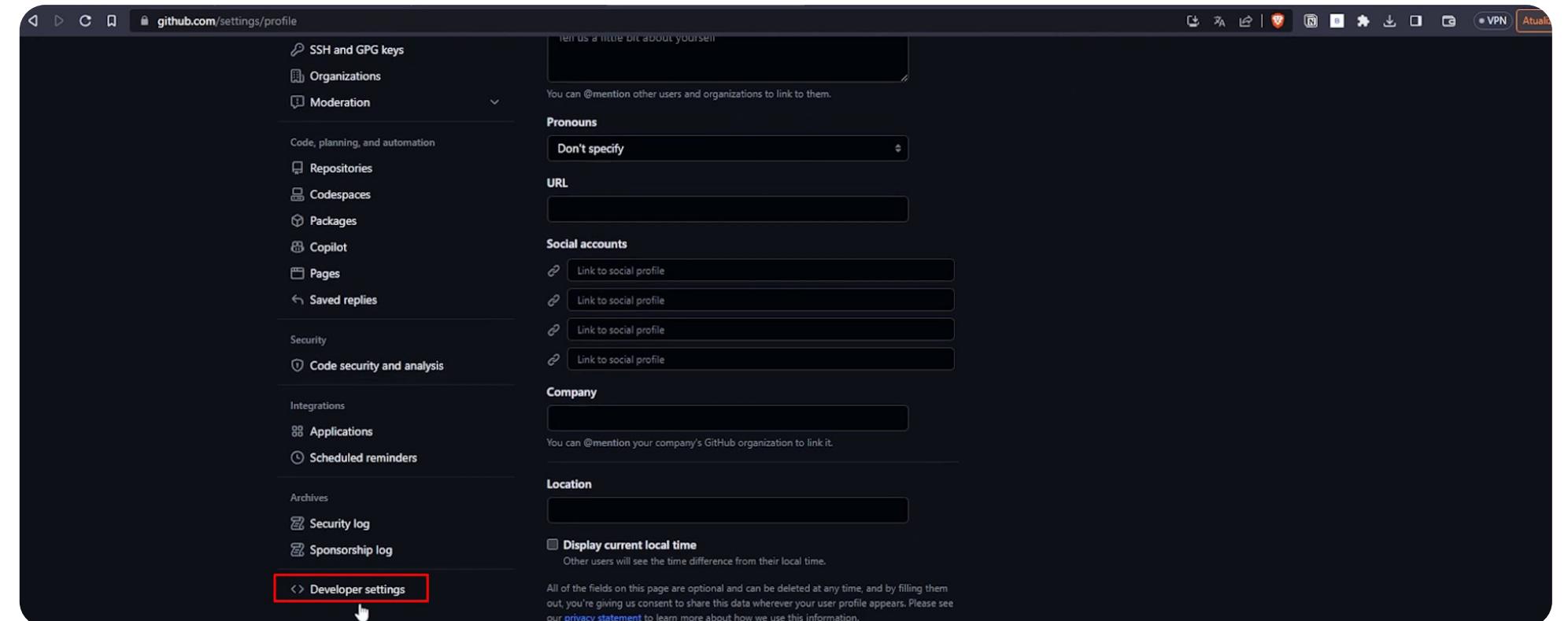
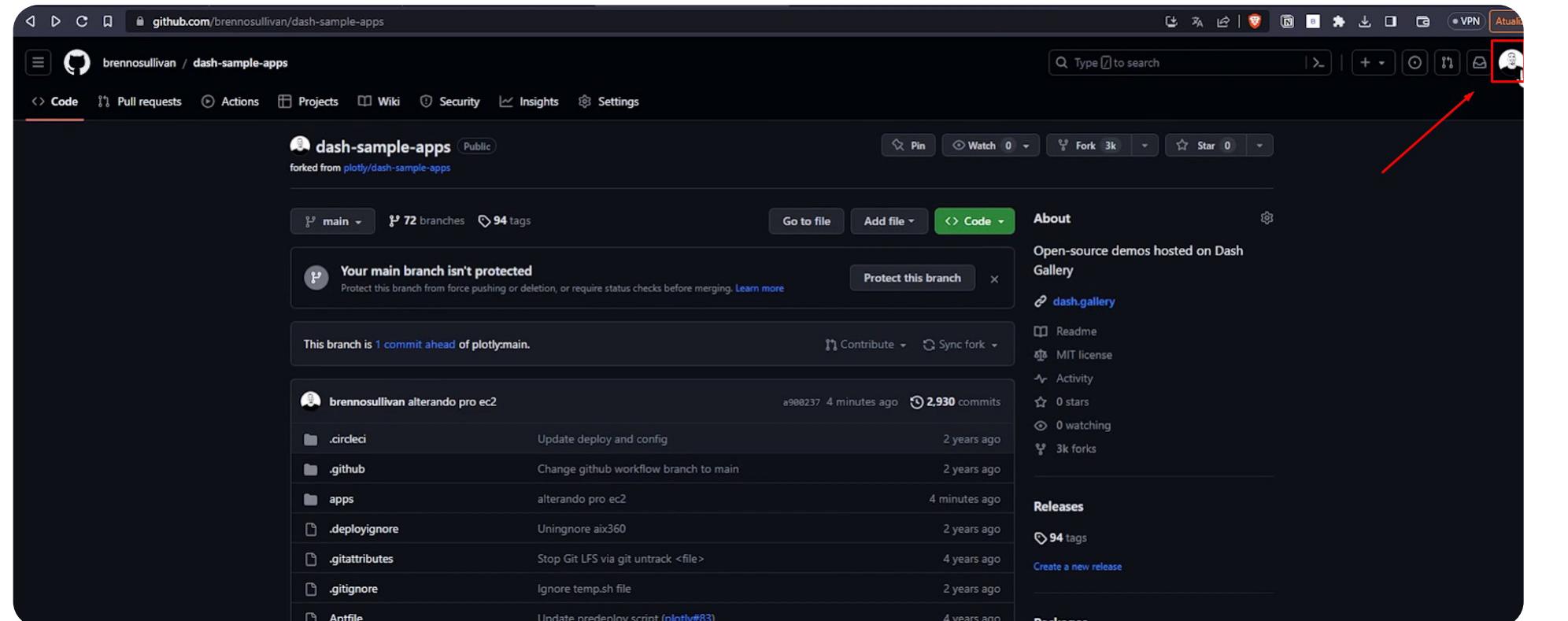
`sudo apt update`

`sudo` é basicamente o administrador do Linux, ou seja, está executando o comando como administrador.

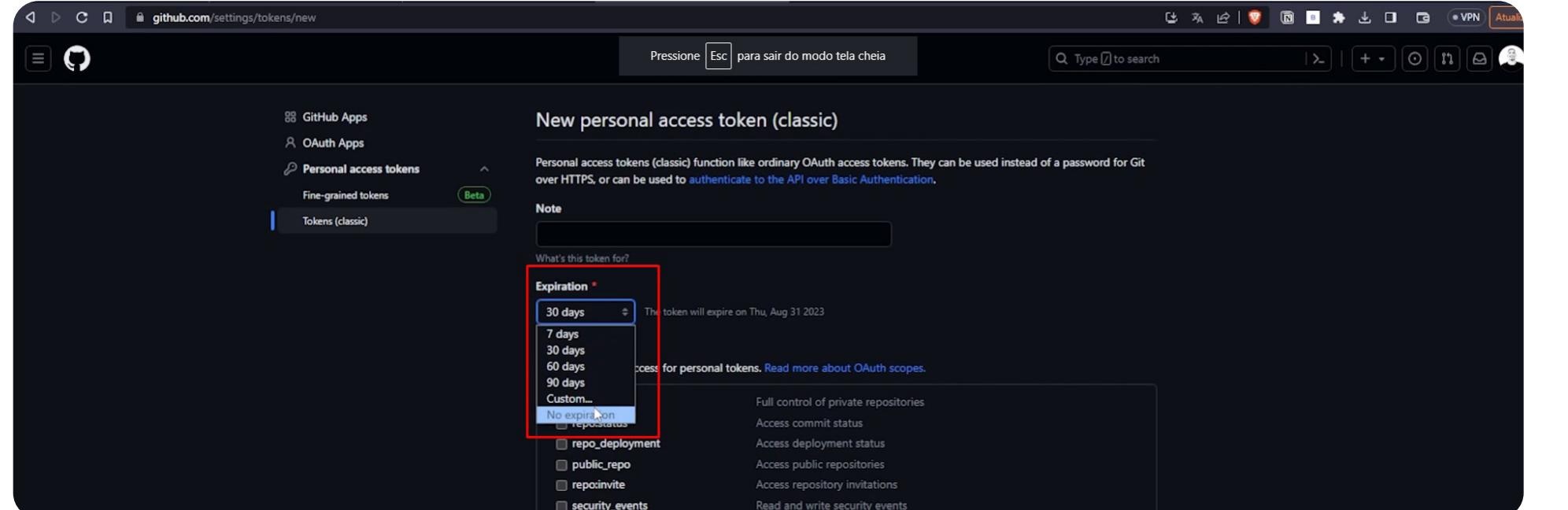
Instalando o Git:

`sudo apt install git`

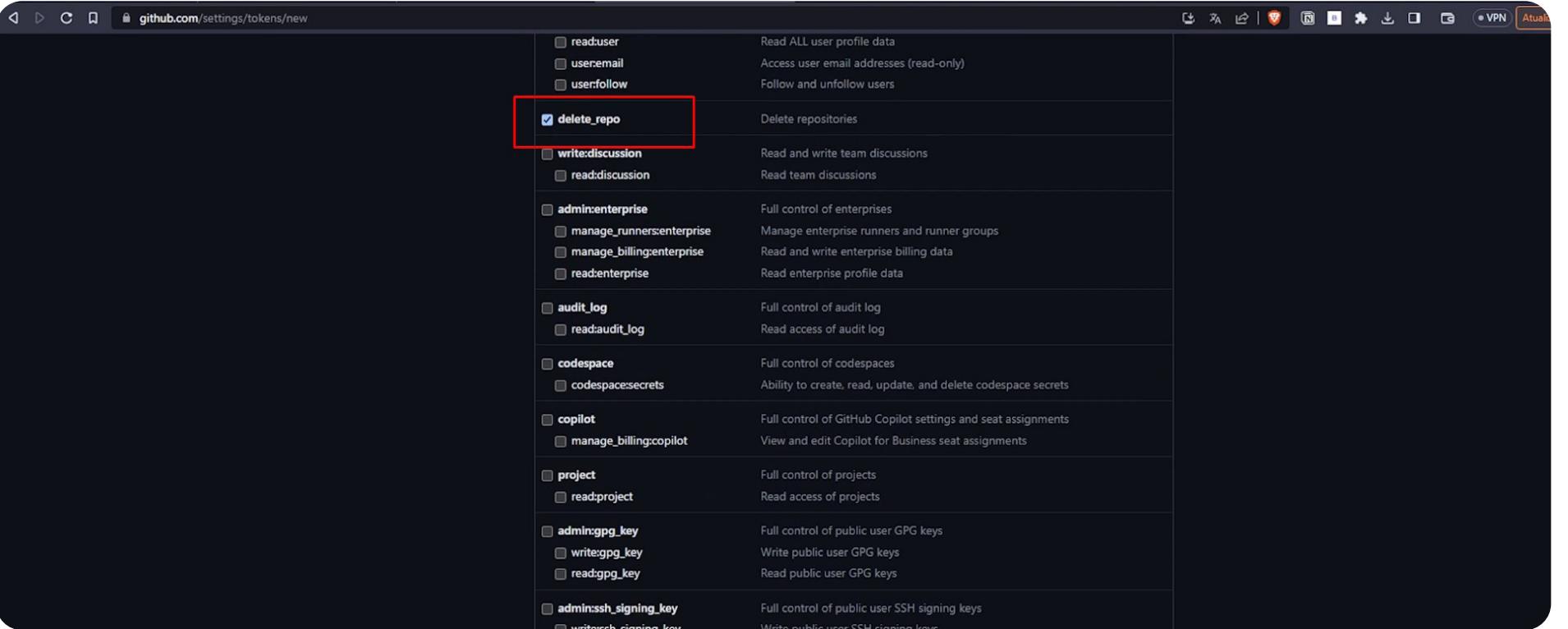
É necessário conectar o EC2 ao GitHub igual na galáxia de GitHub. Configure uma chave SSH pro computador e o GitHub vai atualizar e acessar o repositório.



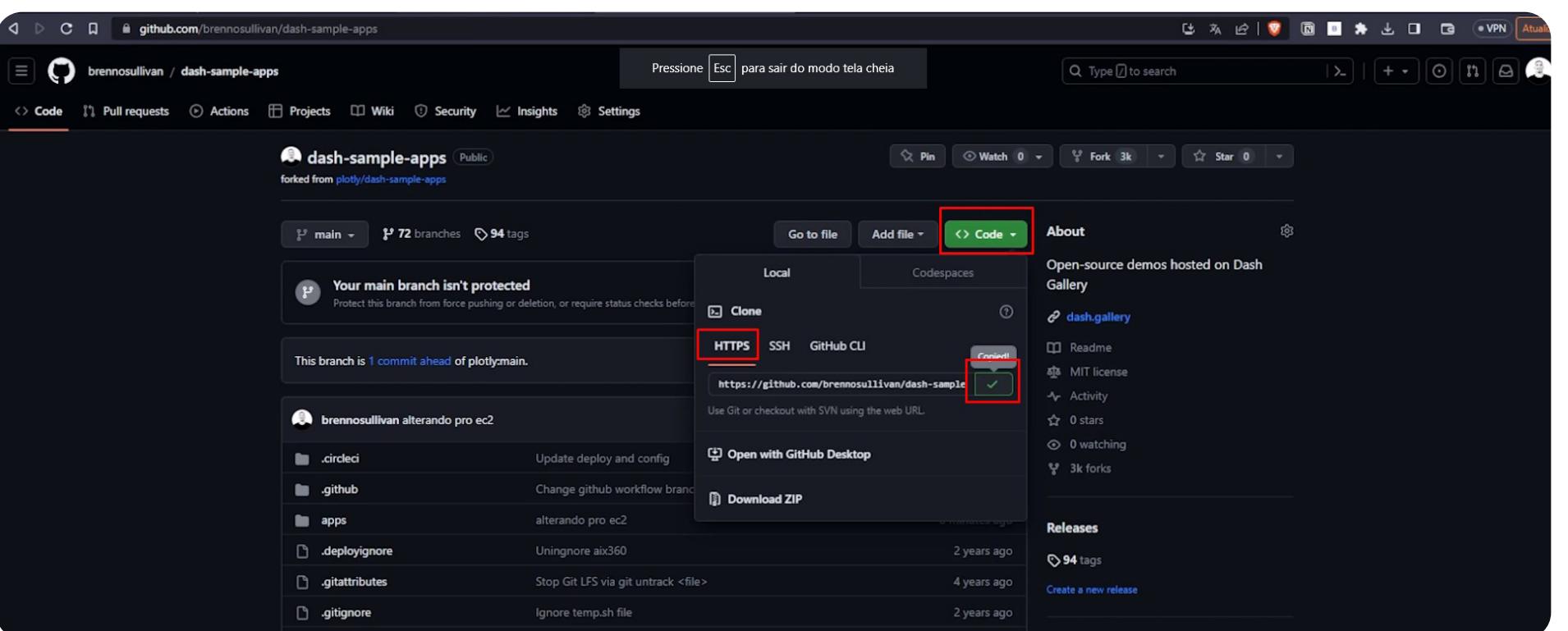
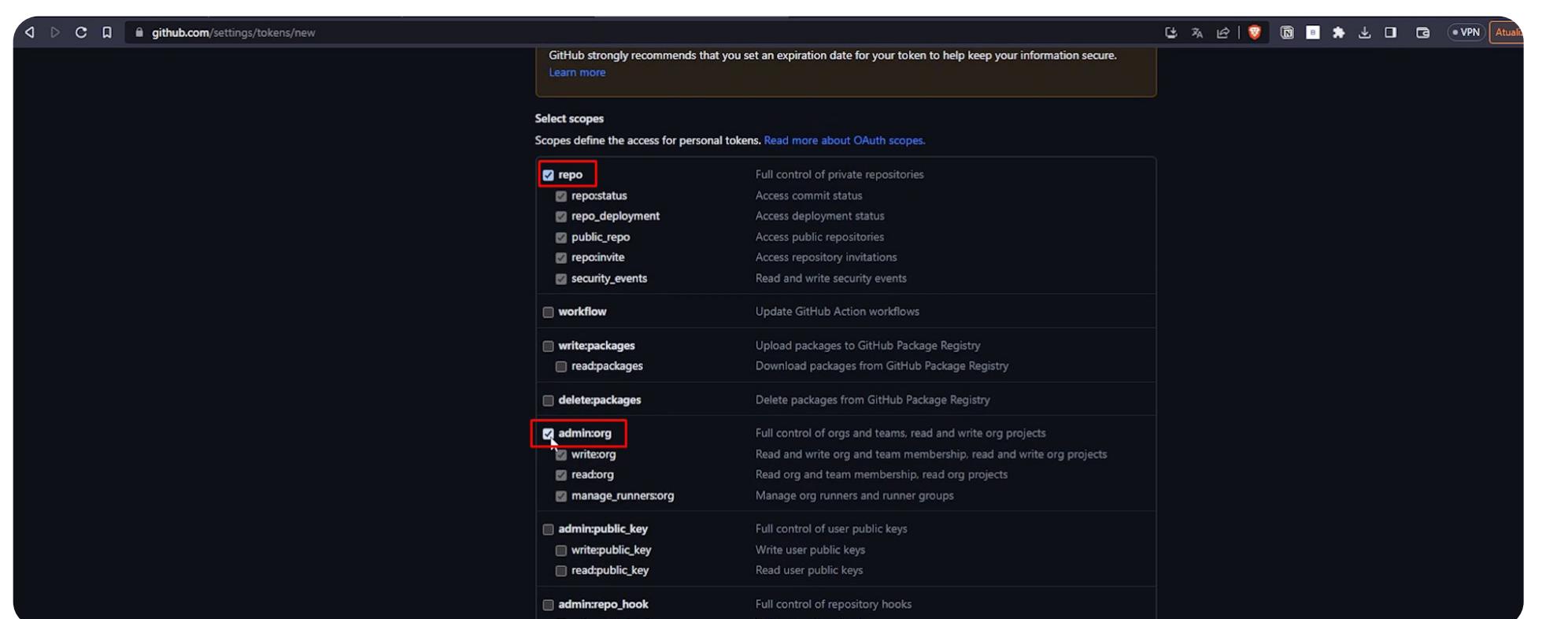
Coloque o seu código de verificação do GitHub, insira um nome para o token, e coloque a data de expiração do token, o ideal é que esse token expire em um tempo razoável.



Descendo a página, selecionaremos o que esse token tem autorização para fazer no GitHub.



Gere o token, guarde a chave, retorne ao GitHub, vá ao projeto do Dash, e cole o link.

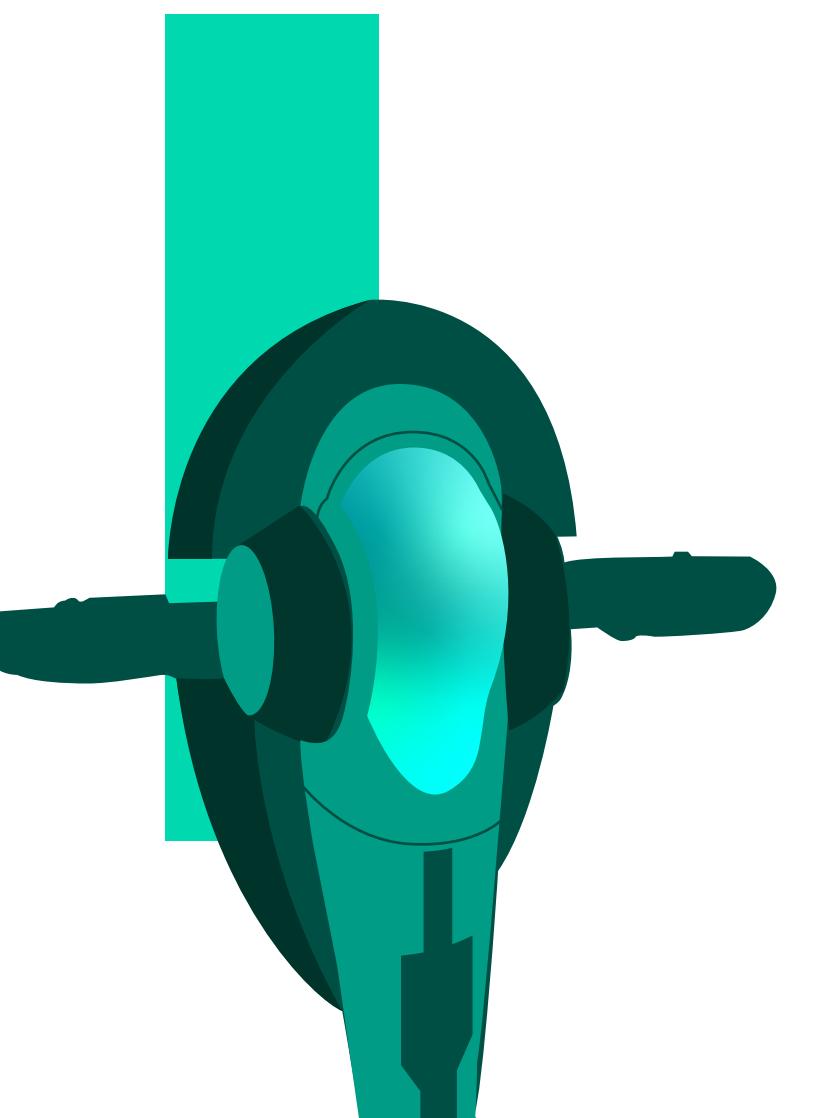


Retorne ao EC2 e digite o seguinte comando no prompt de comando:

```
git clone https://github.com/brennosullivan/dash-sample-apps.git
```

Como você viu, esse comando é para clonar a pasta do dashboard selecionado da biblioteca de dash. Lembrando que, essa é a url do seu GitHub, e para colar é com as teclas de atalho **ctrl+shift+v**, para não bugar, ao invés do padrão **ctrl+v**. Após essa etapa, será solicitado o login e senha, digite o nome do seu usuário no GitHub (login) e o token gerado (senha).

Para confirmar o upload do dash, digite o comando "ls".



```
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [22.2 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [15.4 kB]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [580 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [647 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [152 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [11.0 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [656 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [104 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [532 B]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [767 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [138 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [16.3 kB]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [36.5 kB]
Get:41 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [7060 B]
Get:42 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [260 B]
Fetched 26.4 MB in 5s (5605 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-10-0-3-197:~$ sudo apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.34.1-1ubuntu1.9).
git set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 94 not upgraded.
ubuntu@ip-10-0-3-197:~$ git --version
git version 2.34.1
ubuntu@ip-10-0-3-197:~$ git clone https://github.com/brennosullivan/dash-sample-apps.git
Cloning into 'dash-sample-apps'...
remote: Enumerating objects: 36959, done.
remote: Counting objects: 100% (770/770), done.
remote: Compressing objects: 100% (213/213), done.
remote: Total 36959 (delta 678), reused 601 (delta 554), pack-reused 36189
Receiving objects: 100% (36959/36959), 910.83 MiB | 28.00 MiB/s, done.
Resolving deltas: 100% (19171/19171), done.
Updating files: 100% (1821/1821), done.
ubuntu@ip-10-0-3-197:~$ ls
dash-sample-apps
ubuntu@ip-10-0-3-197:~$ █
```

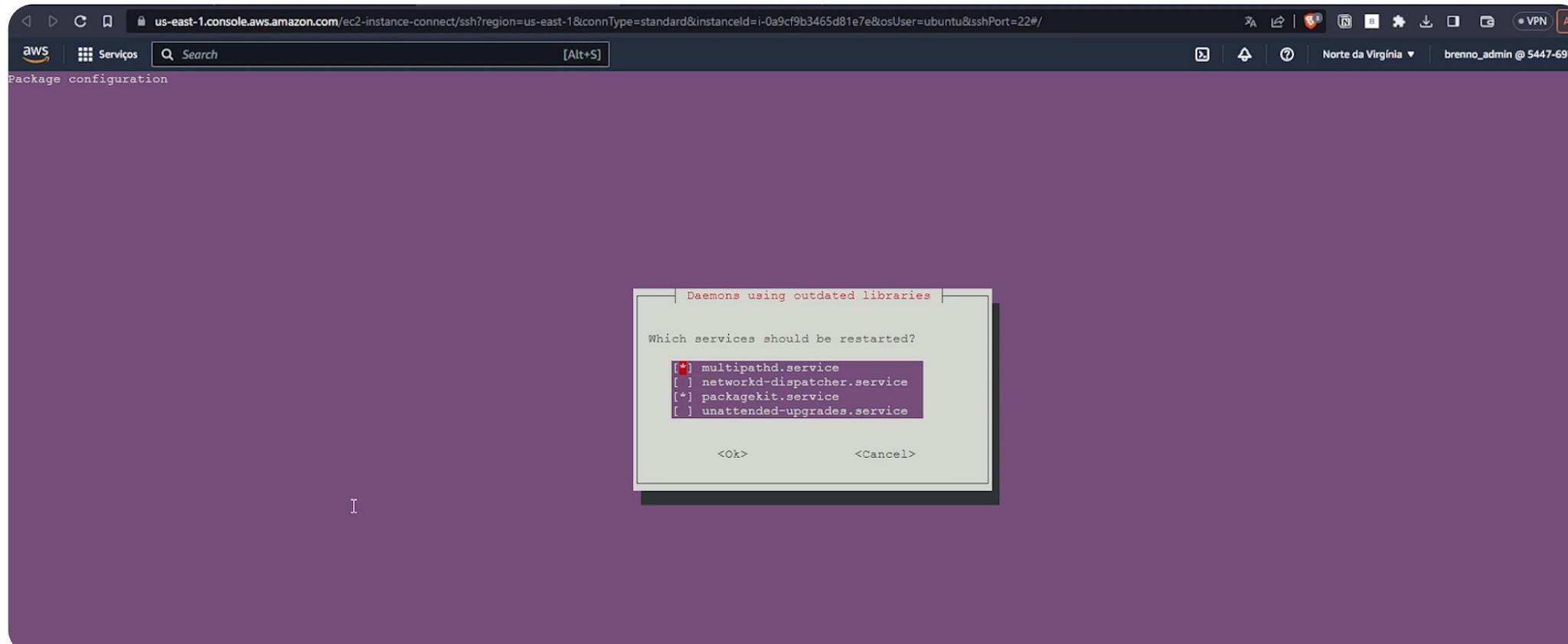
Agora entraremos no diretório para rodar o seu projeto, digitando:

```
cd dash-sample-apps
```

Depois, é necessário baixar tudo que rodará no dashboard dentro da máquina, seja as dependências, pacotes e etc. No próprio ubuntu já vem com o python instalado, mas precisaremos baixar o pip install, e depois instalar os pacotes.

```
sudo apt install python3-pip
```

Caso dê tela roxa, não é nenhum erro, apenas aperte "Enter".



Para a instalação dos pacotes, temos que verificar quais os pacotes que nosso dashboard precisará para rodar perfeitamente. Geralmente, no requirements.txt tem os pacotes necessários para executar o projeto, nesse caso em específico, foi feito um requirementes.txt para cada dashboard separadamente.

Via de regra, essa é a localização.

This branch is 1 commit ahead of plotly:main.	
	brennosullivan alterando pro ec2
	a900237 12 minutes ago 2,930 commits
	.circleci Update deploy and config 2 years ago
	.github Change github workflow branch to main 2 years ago
	apps alterando pro ec2 12 minutes ago
	.deployignore Uningnore aix360 2 years ago
	.gitattributes Stop Git LFS via git untrack <file> 4 years ago
	.gitignore Ignore temp.sh file 2 years ago
	Aptfile Update predeploy script (plotly#83) 4 years ago
	CONTRIBUTING.md Create CONTRIBUTING.md 2 years ago
	LICENSE Create LICENSE 4 years ago
	README.md Correct a typo 2 years ago
	app.json mono-repo skeleton 4 years ago
	deploy Update deploy 2 years ago
	init.R Update predeploy script (plotly#83) 4 years ago
	predeploy.py fix: drop unused variable 4 years ago
	requirements.txt clear requirements.txt 4 years ago
	runtime.txt Revert "DashR Wind Streaming (plotly#162)" 4 years ago

Mas, como no dash, é um para cada dashboard.

This screenshot shows a GitHub repository page for 'dash-sample-apps'. The main directory contains several subfolders labeled 'apps'. One specific folder, 'apps', is highlighted with a red box. The repository has 2,930 commits and 3k forks. It includes sections for 'Gallery', 'Releases', and 'Languages'.

This screenshot shows the contents of the 'dash-clinical-analytics' folder within the 'dash-sample-apps' repository. The folder structure includes 'assets', 'data', 'img', 'Profile', 'README.md', 'app.py', and 'requirements.txt'. The 'requirements.txt' file is highlighted with a red box.

Esses são os pacotes necessários.

This screenshot shows the contents of the 'dash-clinical-analytics' folder within the 'dash-sample-apps' repository. The folder structure includes 'dash-brain-connectivity', 'dash-brain-viewer', 'dash-canvas-ocr', 'dash-chatbot', 'dash-chess-analytics', 'dash-clinical-analytics', 'dash-covid-xray', 'dash-cytoscape-editor', 'dash-cytoscape-ida', 'dash-cytoscape-phylogeny', 'dash-cytoscape', 'dash-daq-iv-tracer', 'dash-daq-satellite-dashboard', 'dash-daq-tektronix350', and 'dash-dashader'. The 'dash-clinical-analytics' folder is highlighted with a red box.

This screenshot shows the contents of the 'dash-clinical-analytics' folder within the 'dash-sample-apps' repository. The folder structure includes 'dash-brain-connectivity', 'dash-chess-analytics', 'dash-clinical-analytics', 'dash-covid-xray', 'dash-cytoscape', 'dash-cytoscape-ida', 'dash-cytoscape-phylogeny', 'dash-cytoscape', 'dash-daq-iv-tracer', and 'dash-daq-satellite-dashboard'. The 'requirements.txt' file is highlighted with a red box.

```

dash==1.9.0
gunzip==0.9.0
numpy==1.16.2
pandas==0.24.2
detelme==4.3
pathlib==1.4.1
    
```

Portanto, vamos modificar o diretório para o dash-clinical-analytics, pois nosso requirement.txt está lá.

```
cd ./apps/dash-clinical-analytics
```

E por fim:

```
sudo pip install -r requirements.txt
```

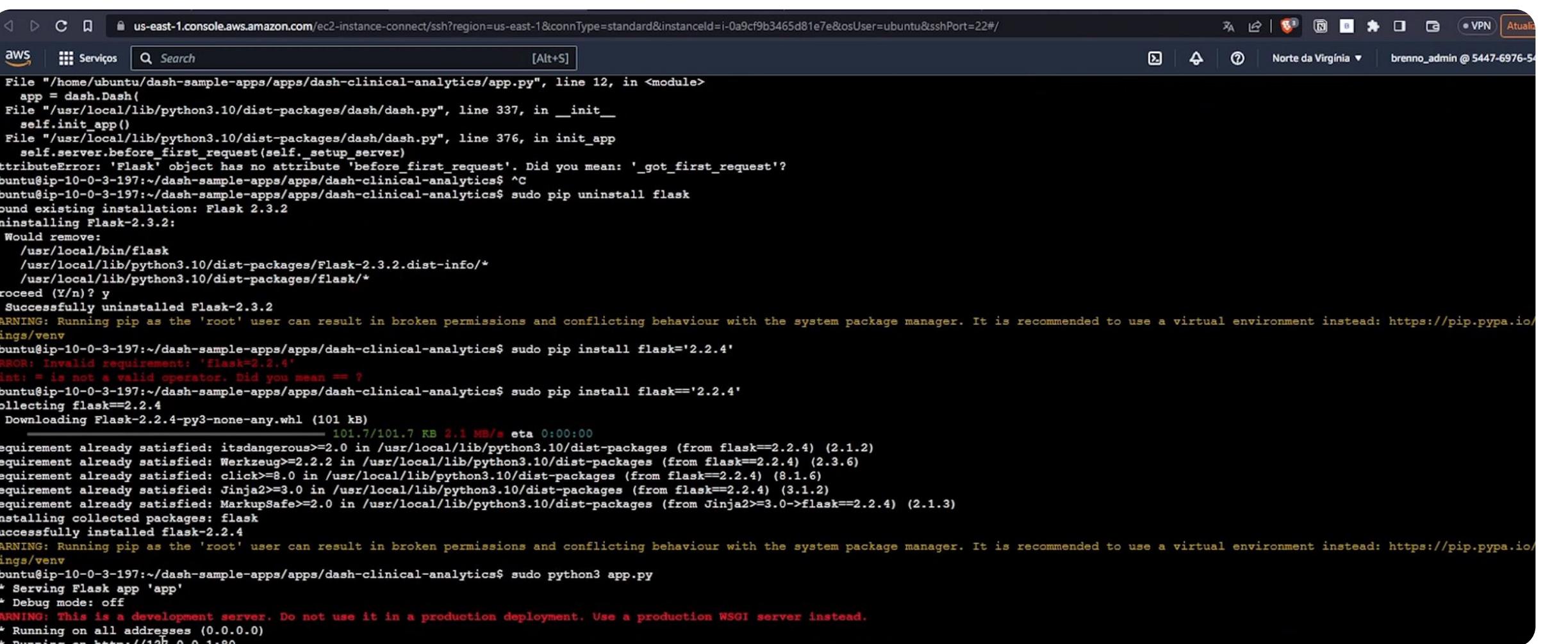
Adiantando um erro, no requirements está configurado errado e não informa a versão correta. O pacote está na versão errada, a versão correta para rodar esse código é a 2.2.4, portanto, desinstalamos o pacote e instalaremos na versão correta. Como descobrir? Jogue o erro no google e descubra.

```
sudo pip uninstall flask
```

```
sudo pip install flask=='2.2.4'
```

Hora de testar se o projeto está rodando:

```
sudo python3 app.py
```

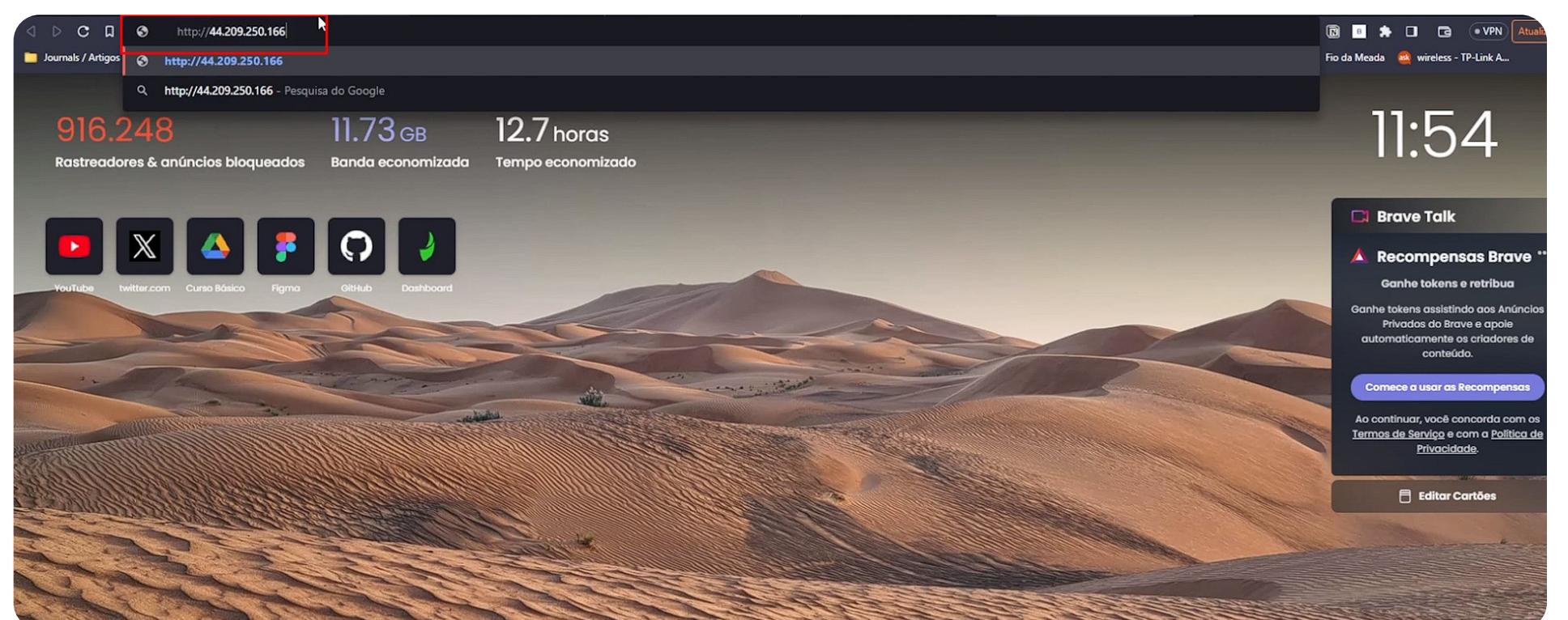


```
File "/home/ubuntu/dash-sample-apps/apps/dash-clinical-analytics/app.py", line 12, in <module>
    app = dash.Dash()
  File "/usr/local/lib/python3.10/dist-packages/dash/dash.py", line 337, in __init__
    self._init_app()
  File "/usr/local/lib/python3.10/dist-packages/dash/dash.py", line 376, in _init_app
    self.server.before_first_request(self._setup_server)
AttributeError: 'Flask' object has no attribute 'before_first_request'. Did you mean: '_got_first_request'?
ubuntu@ip-10-0-3-197:~/dash-sample-apps/apps/dash-clinical-analytics$ ^C
ubuntu@ip-10-0-3-197:~/dash-sample-apps/apps/dash-clinical-analytics$ sudo pip uninstall flask
Found existing installation: Flask 2.3.2
Uninstalling Flask-2.3.2:
Would remove:
  /usr/local/bin/flask
  /usr/local/lib/python3.10/dist-packages/Flask-2.3.2.dist-info/*
  /usr/local/lib/python3.10/dist-packages/flask/*
Proceed (Y/n)? y
Successfully uninstalled Flask-2.3.2
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/
nings/venv
ubuntu@ip-10-0-3-197:~/dash-sample-apps/apps/dash-clinical-analytics$ sudo pip install flask=='2.2.4'
Requirement already satisfied: itsdangerous>=2.0 in /usr/local/lib/python3.10/dist-packages (from flask==2.2.4) (2.1.2)
Requirement already satisfied: Werkzeug>=2.2.2 in /usr/local/lib/python3.10/dist-packages (from flask==2.2.4) (2.3.6)
Requirement already satisfied: click>=8.0 in /usr/local/lib/python3.10/dist-packages (from flask==2.2.4) (8.1.6)
Requirement already satisfied: Jinja2>=3.0 in /usr/local/lib/python3.10/dist-packages (from flask==2.2.4) (3.1.2)
Requirement already satisfied: MarkupSafe>=2.0 in /usr/local/lib/python3.10/dist-packages (from Jinja2>=3.0->flask==2.2.4) (2.1.3)
Installing collected packages: flask
Successfully installed flask-2.2.4
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/
nings/venv
ubuntu@ip-10-0-3-197:~/dash-sample-apps/apps/dash-clinical-analytics$ sudo python3 app.py
* Serving Flask app "app"
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
  Running on http://127.0.0.1:5000
```

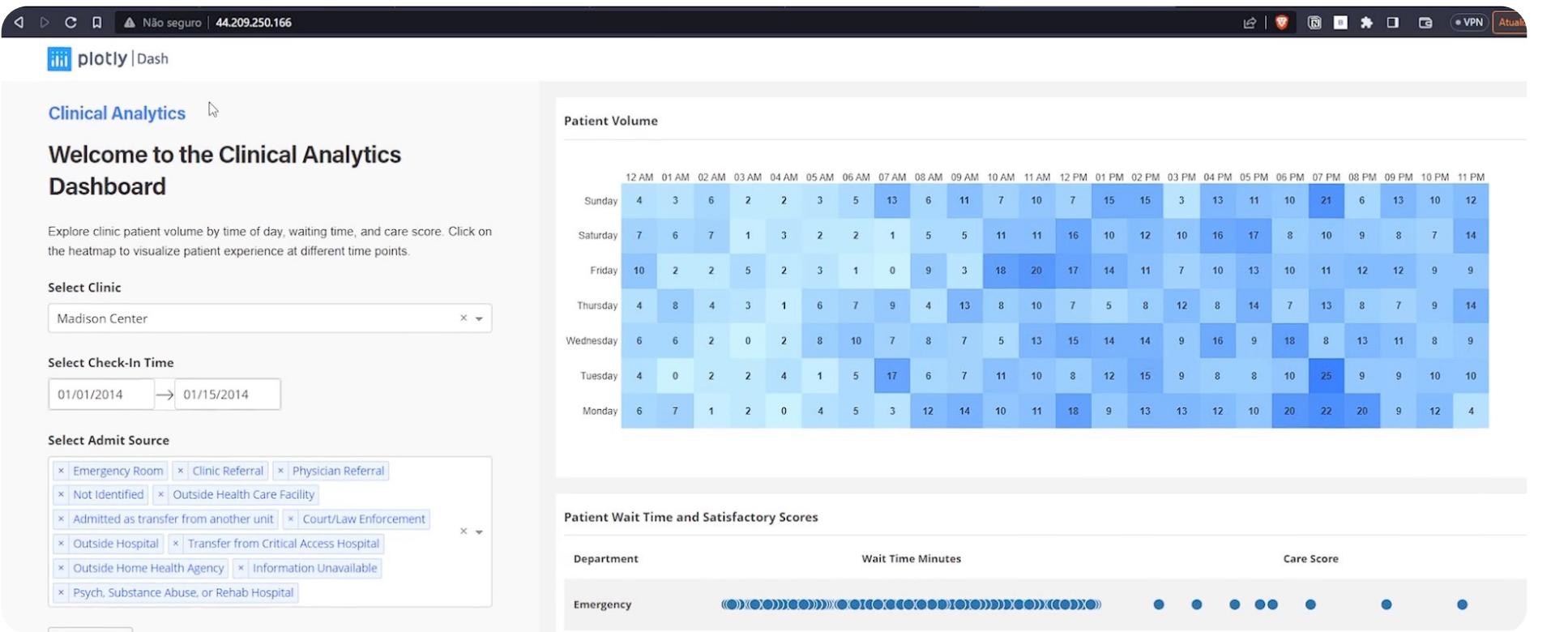
O projeto está rodando! Pegamos o IP Público para acessar o nosso dashboard online.

The screenshot shows the AWS Management Console interface for the EC2 service. In the main list of instances, one instance named "EC2 Dashboard..." is selected, and its details are shown in the bottom pane. The public IP address, 44.209.250.166, is highlighted with a red box in the "Endereço IP público" column.

Não esqueça de colocar o "http://" antes.



DASHBOARD NO AR!



Contudo, o dashboard será mantido no ar somente quando a EC2 estiver sendo executada, pois está rodando em 1º plano, e precisamos modificar para rodar em 2º plano, ou quando finalizar a EC2, não será possível acessar ao dashboard online. Vamos resolver este problema!

Primeiramente, desligue a instância em "Interromper" e não "Encerrar", se não, tudo feito até este momento será jogado por água abaixo.

The screenshot shows the AWS EC2 Instances page. There are two instances listed: 'EC2 Dashboard...' (running, t2.micro, 2/2 verificações aprovadas, Sem alarmes, us-east-1c) and 'EC2 Teste' (terminated, t2.micro, Encerrado, Sem alarmes, us-east-1c). The 'Actions' dropdown menu for the running instance is open, with the 'Interromper instância' option highlighted.

Após a instância ser interrompida...

The screenshot shows the AWS EC2 Instances page after one instance has been terminated. The 'Actions' dropdown menu for the terminated instance 'EC2 Teste' is open, with the 'Configurações de instância' option highlighted.

Copie e cole este código abaixo, conforme o passo a passo. Como já foi dito algumas vezes, há códigos que não escrevemos e simplesmente copiamos pela internet, esse é um desses códigos:

Content-Type: multipart/mixed; boundary="//"

MIME-Version: 1.0

--//

Content-Type: text/cloud-config; charset="us-ascii"

MIME-Version: 1.0

Content-Transfer-Encoding: 7bit

Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config

cloud_final_modules:

- [scripts-user, always]

--//

Content-Type: text/x-shellscrip; charset="us-ascii"

MIME-Version: 1.0

Content-Transfer-Encoding: 7bit

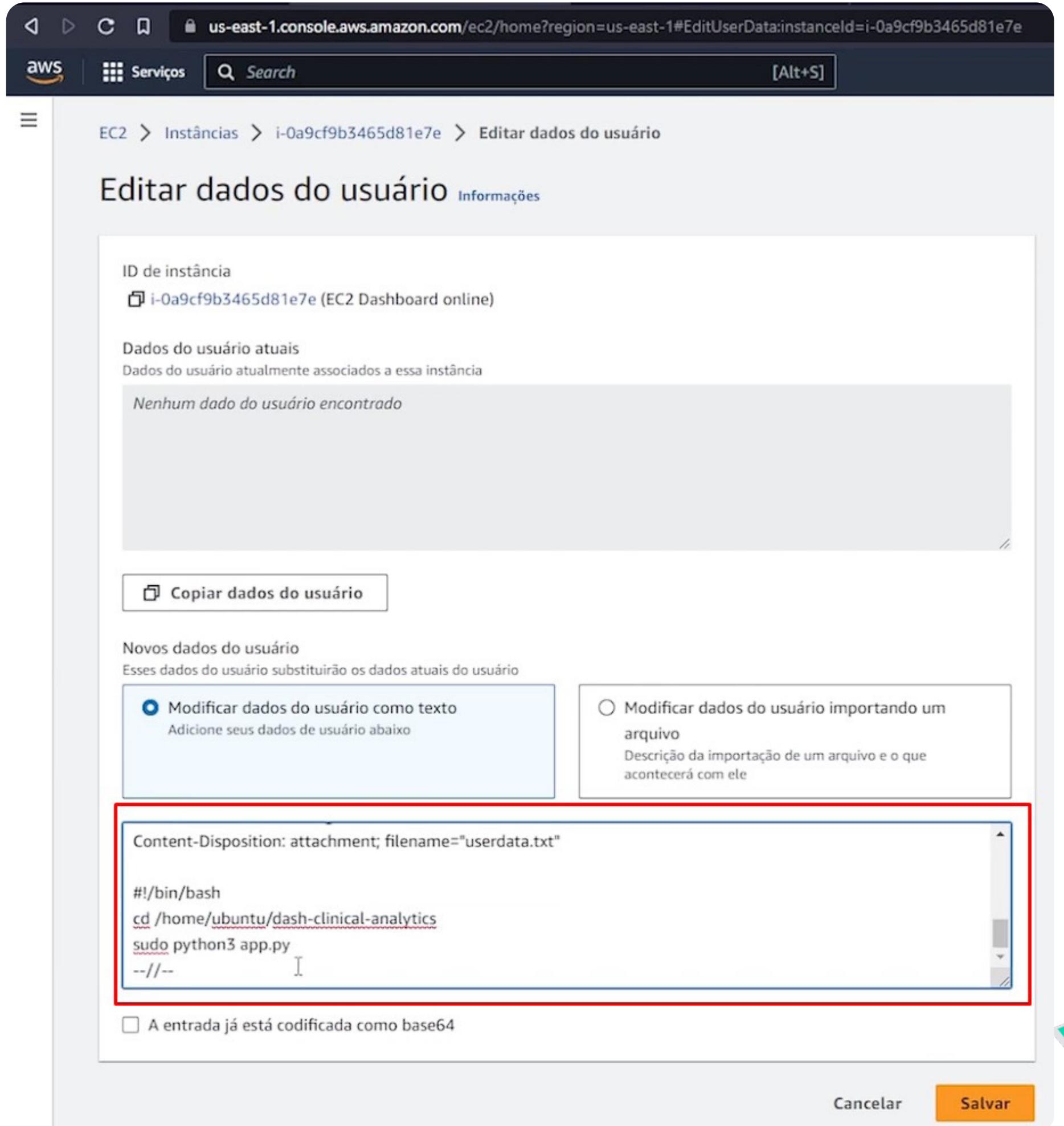
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash

cd /home/ubuntu/dash-sample-apps/apps/dash-clinical-analytics

sudo python3 app.py

--//--

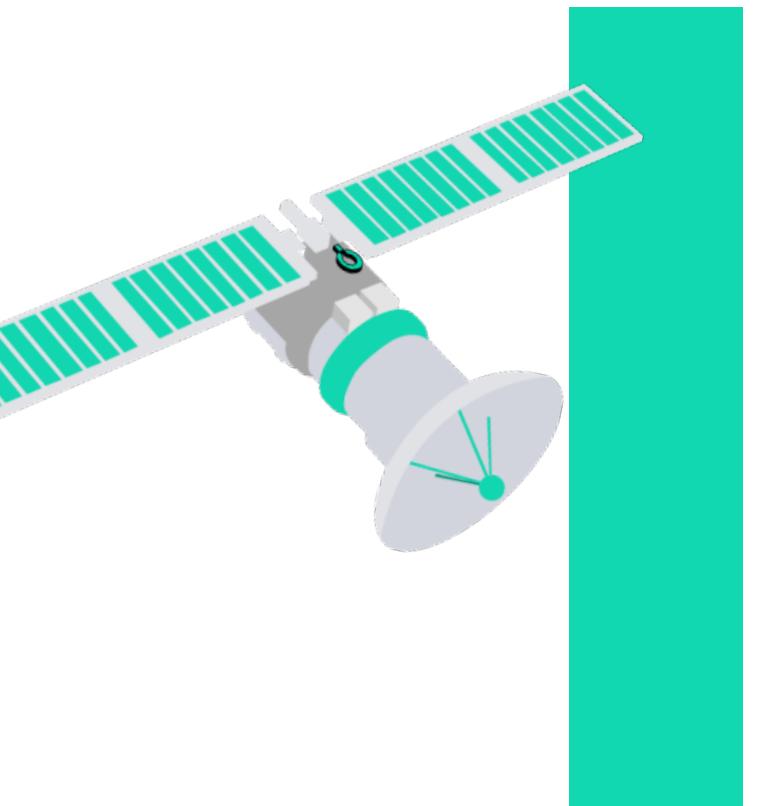


The screenshot shows the 'Editar dados do usuário' (Edit User Data) page in the AWS Management Console. At the top, it displays the instance ID: i-0a9cf9b3465d81e7e. Below this, there's a section for 'ID de instância' (Instance ID) with a link to the EC2 Dashboard online. Under 'Dados do usuário atuais' (Current User Data), it says 'Nenhum dado do usuário encontrado' (No user data found). A 'Copiar dados do usuário' (Copy User Data) button is available. In the 'Novos dados do usuário' (New User Data) section, two options are shown: 'Modificar dados do usuário como texto' (Modify user data as text) and 'Modificar dados do usuário importando um arquivo' (Modify user data by importing a file). The 'Modificar dados do usuário como texto' option is selected. Below this, a text area contains a terminal script:

```
Content-Disposition: attachment; filename="userdata.txt"
#!/bin/bash
cd /home/ubuntu/dash-clinical-analytics
sudo python3 app.py
--/--
```

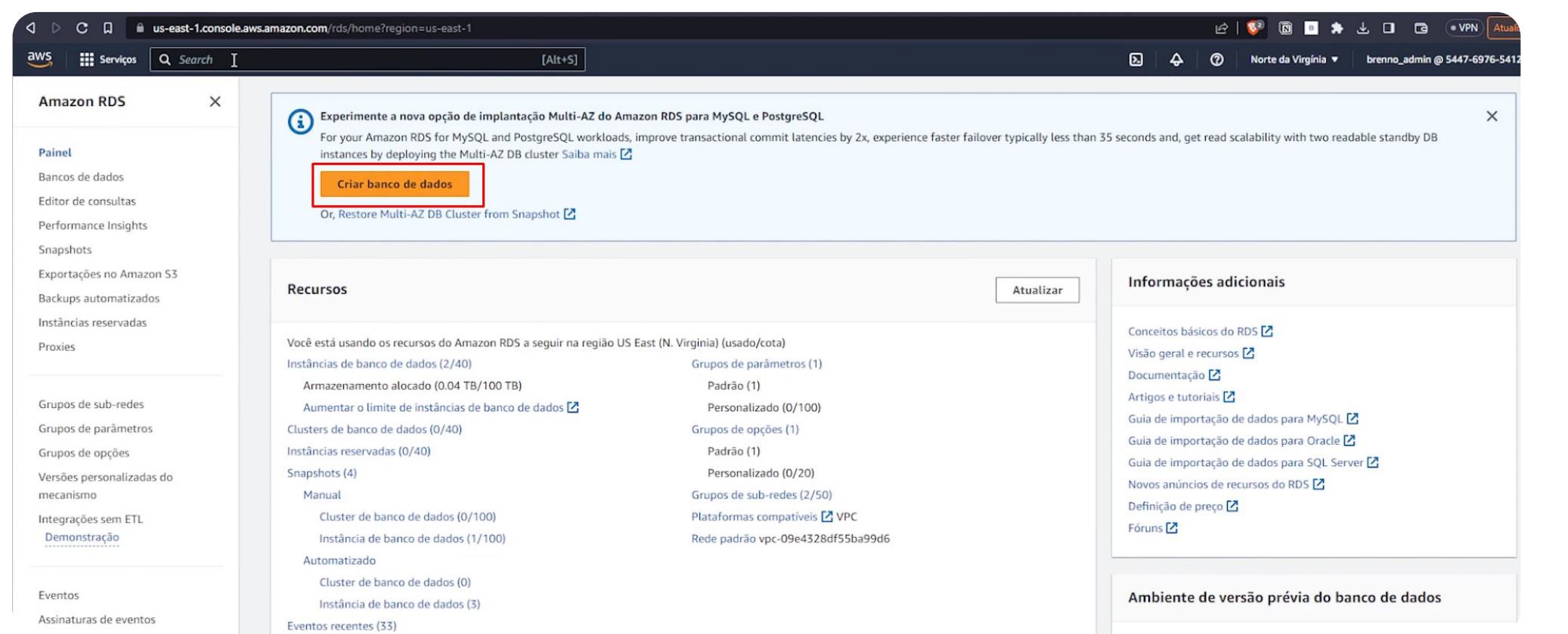
A checkbox 'A entrada já está codificada como base64' (The input is already encoded as base64) is present. At the bottom are 'Cancelar' (Cancel) and 'Salvar' (Save) buttons.

Depois initialize a instância, aguarde o delay, e o dashboard está no ar rodando em 2º plano.

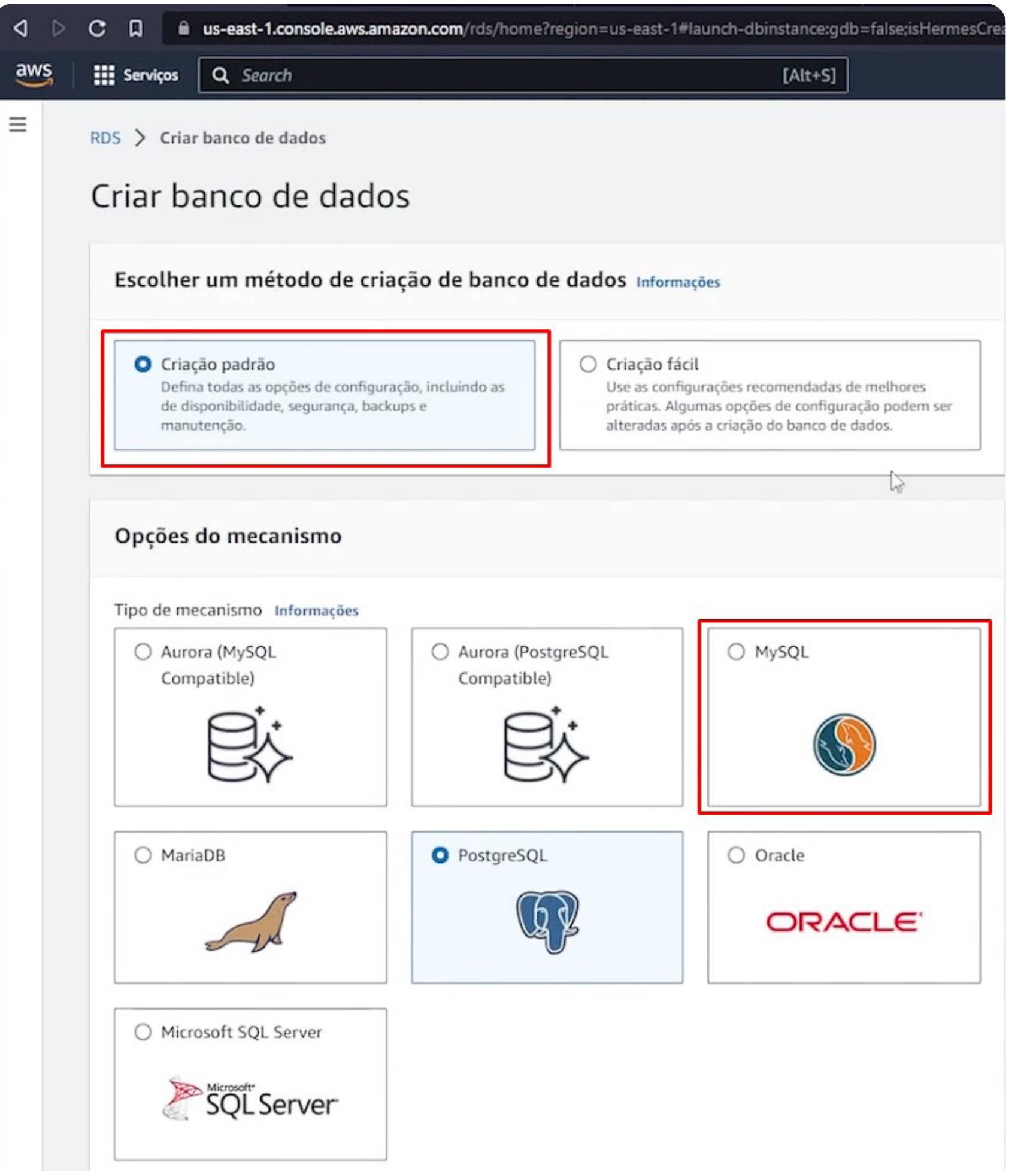


Projeto 2: Banco de dados na nuvem

Esse projeto será voltado para a criação de banco de dados na AWS. Para isso, procure o serviço “RDS”, assim como procuramos os serviços de EC2, VPC e etc.



The screenshot shows the AWS RDS console interface. On the left, there's a sidebar with various options like Painel, Bancos de dados, and Snapshots. The main area displays resource statistics such as 'Instâncias de banco de dados (2/40)', 'Clusters de banco de dados (0/40)', and 'Schemas (4)'. A prominent orange button labeled 'Criar banco de dados' is located at the top right of the main content area, which is highlighted with a red box.



The screenshot shows the 'Criar banco de dados' (Create Database) wizard. The first step, 'Escolher um método de criação de banco de dados', is displayed. It offers two options: 'Criação padrão' (selected, highlighted with a red box) and 'Criação fácil'. Below these, the 'Opções do mecanismo' (Mechanism Options) section is shown, featuring icons and names for various databases: Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible), MySQL (selected, highlighted with a red box), MariaDB, PostgreSQL (selected), Oracle, and Microsoft SQL Server.

Utilize a versão mais atualizada e o nível gratuito.

The screenshot shows the 'Create New DB Instance' wizard. In the 'Mechanism Version' section, 'MySQL 8.0.33' is selected. In the 'Instance Type' section, 'Nível gratuito' (Free tier) is selected. Both sections are highlighted with red boxes.

Escolha um nome para a instância do seu banco de dados, ao configurar as credenciais, pode manter como padrão “admin”, e crie sua senha.

The screenshot shows the 'Create New DB Instance' wizard. In the 'Database Identifier' section, 'codigopyteste' is entered into the input field. In the 'User Credentials' section, 'admin' is entered into the 'Nome do usuário principal' field. Both fields are highlighted with red boxes.

Escolha sua instância, no caso, seu computador. Os computadores disponíveis estão limitados ao free-tier.

Configuração da instância

As opções de configuração da instância de banco de dados abaixo são limitadas àquelas compatíveis com o mecanismo selecionado acima.

Gravações otimizadas do Amazon RDS - novo [Informações](#)

Mostrar classes de instância compatíveis com gravações otimizadas do Amazon RDS

Classe da instância de banco de dados [Informações](#)

Classes padrão (inclui classes m)

Classes otimizadas para memória (inclui classes r e x)

Classes com capacidade de intermitência (inclui classes t)

db.t3.micro
2 vCPUs 1 GiB RAM Rede: 2.085 Mbps

Incluir as classes de geração anteriores

Armazenamento

Tipo de armazenamento [Informações](#)

SSD de uso geral (gp2)
Performance de linha de base determinada pelo tamanho do volume

Armazenamento alocado [Informações](#)

20 GiB
O valor mínimo é 20 GiB e o valor máximo é 6.144 GiB

After you modify the storage for a DB instance, the status of the DB instance will be in storage-optimization. Your instance will remain available as the storage-optimization operation completes. [Saiba mais](#)

Escalabilidade automática do armazenamento [Informações](#)

Fornecer suporte à escalabilidade dinâmica do seu armazenamento de banco de dados de acordo com as necessidades do seu aplicativo.

Habilitar escalabilidade automática do armazenamento
Habilitar esse recurso permite que o armazenamento aumente depois que o limite especificado for excedido.

Limite máximo de armazenamento [Informações](#)

As cobranças serão aplicadas quando seu banco de dados escalar automaticamente para o limite especificado

1000 GiB
O valor mínimo é 22 GiB e o valor máximo é 6.144 GiB

Quanto ao armazenamento, 20gb é o máximo do plano free-tier.

Quanto à escalabilidade, refere-se à capacidade da AWS aumentar o armazenamento disponível sem intervenção manual, quando necessário, para atender as necessidades do banco de dados. Lembrando que acima de 20gb, a AWS inicia a cobrança.

Ao conectar-se na EC2, está havendo uma camada a mais de segurança para a conexão ao banco de dados. Ou seja, só conseguiria acessar o banco de dados através da EC2. Como esse é um projeto simples, não irá ficar habilitado. Quanto à VPC, escolhemos a que foi criada no mundo 9.

Conectividade [Informações](#)

Recurso de computação

Escolha se deseja configurar uma conexão com um recurso de computação para esse banco de dados. A configuração de uma conexão altera automaticamente as configurações de conectividade, para que o recurso de computação possa se conectar a esse banco de dados.

Não se conectar a um recurso de computação do EC2
Não configure uma conexão com um recurso de computação para esse banco de dados. Você poderá configurar uma conexão com um recurso de computação manualmente mais tarde.

Conectar-se a um recurso de computação do EC2
Configure uma conexão com um recurso de computação do EC2 para esse banco de dados.

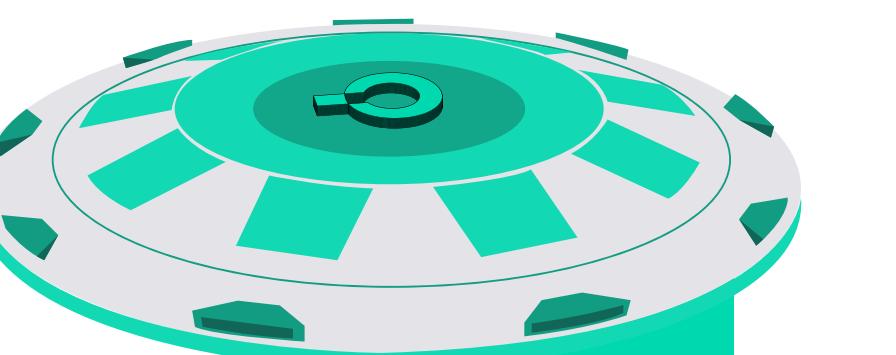
Nuvem privada virtual (VPC) [Informações](#)

Escolha a VPC. A VPC define o ambiente de rede virtual dessa instância de banco de dados.

Default VPC (vpc-09e4328df55ba99d6)
6 Sub-redes, 6 Availability Zones

Somente as VPCs com um grupo de sub-redes de banco de dados correspondente são listadas.

Mesmo liberando o acesso ao público, é necessário um login e uma senha para conectar-se ao banco de dados, diferentemente do projeto de dashboard, que bastava inserir o IP público na url.



Grupo de sub-redes de banco de dados [Informações](#)

Escolha o grupo de sub-redes de banco de dados. O grupo de sub-redes de banco de dados define quais sub-redes e intervalos de IP a instância de banco de dados pode usar na VPC selecionada.

default-vpc-021c195a3b8d2aa78
3 Sub-redes, 3 Availability Zones

Acesso público [Informações](#)

Sim

O RDS atribui um endereço IP público ao banco de dados. As instâncias do Amazon EC2 e outros recursos fora da VPC podem se conectar ao seu banco de dados. Os recursos dentro da VPC também podem se conectar ao banco de dados. Escolha um ou mais grupos de segurança de VPC que especificam quais recursos podem se conectar ao banco de dados.

Não

O RDS não atribui um endereço IP público ao banco de dados. Somente instâncias do Amazon EC2 e outros recursos dentro da VPC podem se conectar ao seu banco de dados. Escolha um ou mais grupos de segurança de VPC que especificam quais recursos podem se conectar ao banco de dados.

Grupo de segurança de VPC (firewall) [Informações](#)

Escolha um ou mais grupos de segurança de VPC para permitir o acesso ao seu banco de dados. Certifique-se de que as regras dos grupos de segurança permitem o tráfego de entrada apropriado.

Selecionar existente
Selecionar grupos de segurança da VPC existentes

Criar novo
Criar grupo de segurança da VPC

Grupos de segurança da VPC existentes

Choose one or more options

default X

Continuando em conectividade, criaremos um novo grupo de segurança, afinal, o ideal é criar um para cada necessidade. Portanto, nomeie, e não existe preferência por zona de disponibilidade. Quanto ao RDS Proxy e Autoridade de certificação, mantenha o padrão.

Grupo de segurança de VPC (firewall) Informações
Escolha um ou mais grupos de segurança de VPC para permitir o acesso ao seu banco de dados. Certifique-se de que as regras dos grupos de segurança permitam o tráfego de entrada apropriado.

Selecionar existente
Selecionar grupos de segurança da VPC existentes

Criar novo
Criar grupo de segurança da VPC

Novo nome do grupo de segurança da VPC
SC - RDS CODIGOPY

Zona de disponibilidade Informações
Sem preferência

RDS Proxy
O RDS Proxy é um proxy de banco de dados totalmente gerenciado e altamente disponível que melhora a escalabilidade, a resiliência e a segurança das aplicações.

Criar um RDS Proxy Informações
O RDS cria automaticamente um perfil do IAM e um segredo do Secrets Manager para o proxy. O RDS Proxy tem custos adicionais. Para obter mais informações, consulte Preços do Amazon RDS Proxy [\[?\]](#).

Autoridade de certificação - opcional Informações
O uso de um certificado de servidor fornece uma camada extra de segurança ao validar que a conexão está sendo feita com um banco de dados da Amazon. Ele faz isso verificando o certificado do servidor instalado automaticamente em todos os bancos de dados provisionados.

rds-ca-2019 (padrão)

Se você não selecionar uma autoridade de certificação, o RDS escolherá uma para você.

Configuração adicional

Novamente uma camada de segurança, você pode escolher o que achar mais seguro, colocaremos “Autenticação de senha”.

Autenticação de banco de dados

Opções de autenticação de bancos de dados Informações

Autenticação de senha
Autentica usando senhas do banco de dados.

Autenticação de senha e do banco de dados do IAM
Autentica usando a senha e as credenciais de usuário do banco de dados por meio de usuários e funções do AWS IAM.

Senha e autenticação Kerberos
Escolha um diretório em que você deseja permitir que usuários autorizados se autentiquem nessa instância de banco de dados usando a Autenticação Kerberos.

Por enquanto, não há necessidade de ativação.

Monitoramento

Monitoramento

Habilitar monitoramento avançado
É útil habilitar métricas de monitoramento avançado quando você deseja ver como diferentes processos ou threads usam a CPU.

Especifique um nome para seu banco de dados, e pode escolher o período que haverá backups, e o tempo em que esse backup será armazenado.

▼ Configuração adicional
Opções de banco de dados, criptografia ativado, backup ativado, retroceder desativado, manutenção, CloudWatch Logs, excluir proteção desativado.

Opções de banco de dados

Nome do banco de dados inicial [Informações](#)
testecodigopy
Se você não especificar um nome de banco de dados, o Amazon RDS não criará um banco de dados.

Grupo de parâmetros do banco de dados [Informações](#)
default.mysql8.0

Grupo de opções [Informações](#)
default:mysql-8-0

Backup

Habilitar backups automatizados.
Cria um snapshot point-in-time do seu banco de dados

⚠ Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to details here [\[2\]](#).

Período de retenção de backup [Informações](#)
O número de dias (1 a 35) para a retenção dos backups automáticos.
1 dia

Janela de backup [Informações](#)
O intervalo de tempo diário (em UTC) durante o qual o RDS realiza backups automatizados.
 Escolher uma janela
 Sem preferência

Copiar tags para snapshots

Mantenha uma versão padrão e que não poderá ser modificada, ou quebrará seus códigos e banco de dados, devido uma atualização inesperada. E também, habilite a proteção contra exclusão, como o próprio nome informa, é impossível que você ou alguém exclua seu banco de dados.

Manutenção
Upgrade automático de versões secundárias [Informações](#)

Habilitar o upgrade automático da versão secundária
Habilitar os upgrades automáticos de versões secundárias fará upgrade automaticamente para as novas versões secundárias à medida que forem lançadas. Os upgrades automáticos ocorrem durante a janela de manutenção do banco de dados.

Janela de manutenção [Informações](#)
Selecionar o período no qual você deseja que as modificações pendentes ou a manutenção sejam aplicadas ao banco de dados pelo Amazon RDS.

Escolher uma janela
 Sem preferência

Proteção contra exclusão

Habilitar a proteção contra exclusão
Protege o banco de dados de ser excluído acidentalmente. Enquanto essa opção estiver habilitada, você não pode excluir o banco de dados.

Lembrando que esses custos mensais estimados seria apenas para caso não tivesse com o free-tier ativado, o que não é seu caso.

Estimated Monthly costs

Instância de banco de dados	12.41 USD
Armazenamento	2.30 USD
Total	14.71 USD

This billing estimate is based on on-demand usage as described in [Preço do Amazon RDS](#). Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.

Estime seus custos mensais para a instância de banco de dados usando a [Calculadora Mensal da AWS](#).

Custos mensais estimados

O nível gratuito do Amazon RDS ficará disponível para você por 12 meses. A cada mês, o nível gratuito permite o uso gratuito dos recursos do Amazon RDS listados abaixo:

- 750 horas do Amazon RDS em uma instância db.t2.micro, db.t3.micro ou db.t4g.micro Single-AZ.
- 20 GB de armazenamento de uso geral (SSD).
- 20 GB de armazenamento para backup automatizado e qualquer snapshot de banco de dados iniciado pelo usuário.

[Learn more about AWS Free Tier.](#)

When your free usage expires or if your application use exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the [Amazon RDS Pricing page](#).

① Você é responsável por garantir que tem todos os direitos necessários para todos os produtos ou serviços de terceiros usados com os serviços da AWS.

[Cancelar](#) [Criar banco de dados](#)

RDS > Bancos de dados > codigopyteste

Resumo

Identificador do banco de dados codigopyteste	CPU	Status Fazendo backup	Classe db.t3.micro
Função Instância	Atividade atual 0 Conexões	Mecanismo MySQL Community	Região e AZ us-east-1a

Segurança e conexão

Endpoint codigopyteste.cnfidyqmv.us-east-1.rds.amazonaws.com	Redes	Segurança
Zona de disponibilidade us-east-1a	VPC	Grupos de segurança da VPC SC - RDS CODIGO PY (sg-015d74826cd8809ef) Ativo
Porta 3306	Varos VPC (vpc-021c195a3b8d2aa78)	Publicamente acessível

Welcome to MySQL Workbench

MySQL Workbench is the official graphical user interface (GUI) tool for MySQL. It allows you to design, create and browse your database schemas, work with database objects and insert data as well as design and run SQL queries to work with stored data. You can also migrate schemas and data from other database vendors to your MySQL database.

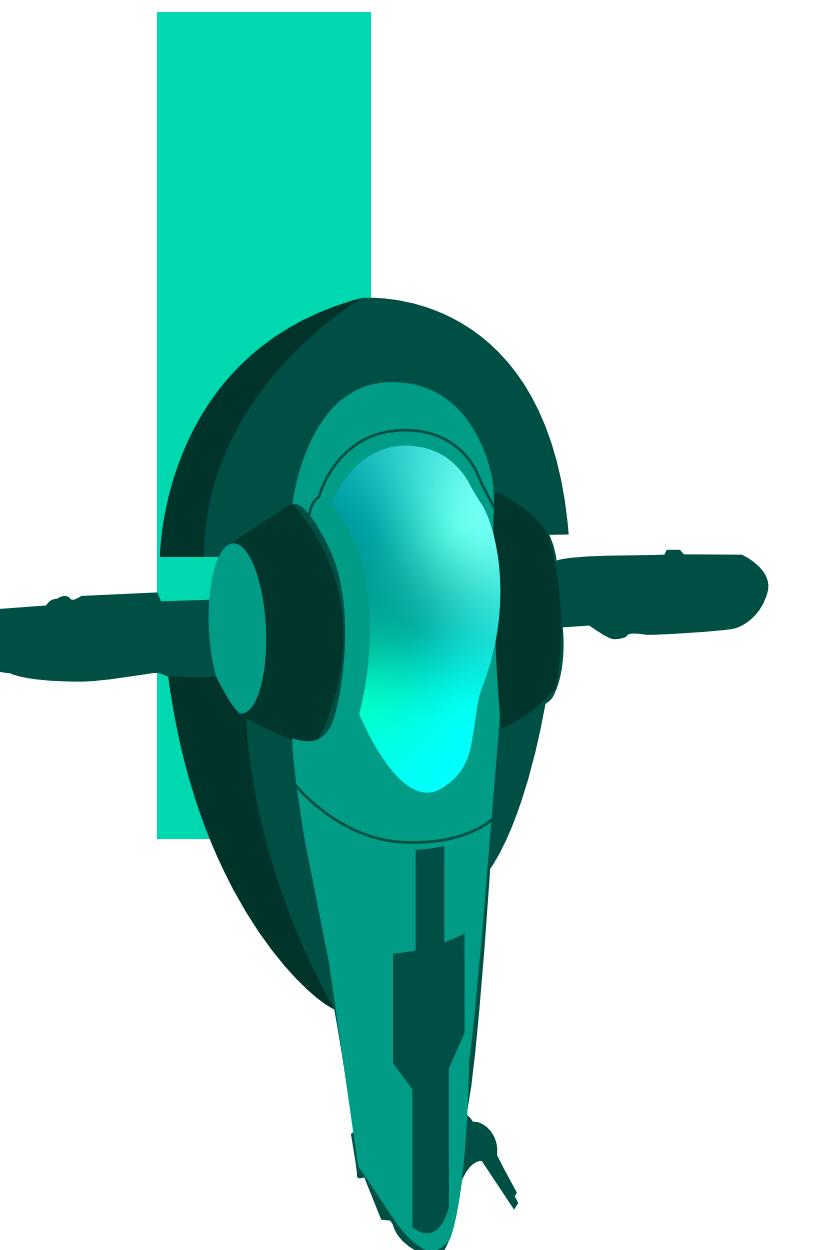
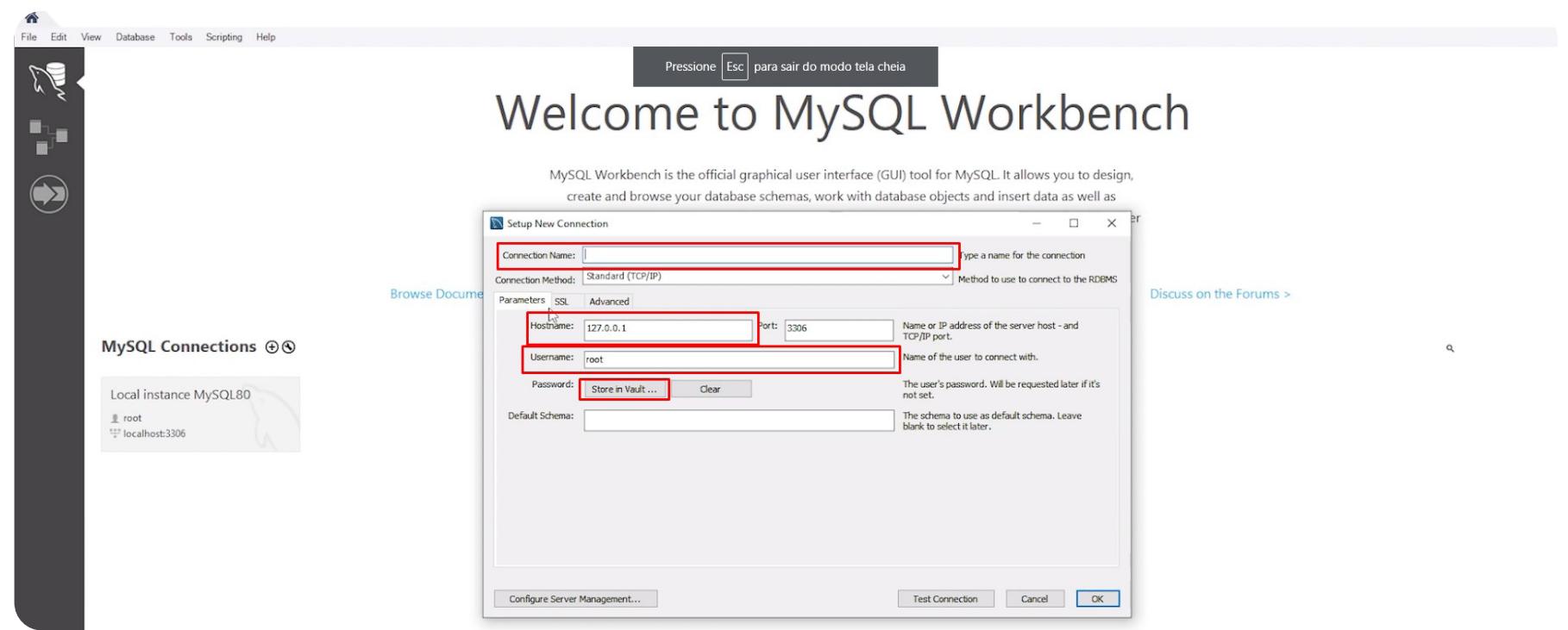
[Browse Documentation >](#) [Read the Blog >](#) [Discuss on the Forums >](#)

MySQL Connections

- Local instance MySQL80
 - root
 - localhost:3306

Pronto, Banco de Dados criado, e essa será seu hostname, ou endpoint.

Preencha todos os campos, com o nome de sua escolha, o hostname (ou endpoint), nome do usuário (havíamos mantido como padrão no início o nome de "admin"), e sua senha criada.



Está finalizado o banco de dados criado na nuvem.

Projeto 3: Automatização de um modelo de investimento

Esse é o maior projeto até o momento, e será ensinado como implementar um algoritmo de trading, conectado diretamente na B³ para automatizar a implementação de qualquer modelo de investimento.

O programa de automatização será colocado dentro da configuração criada na AWS, e o seu modelo de investimento vai rodar 24h por dia, respeitando todos os sinais que você criou, independente se o seu computador estiver ligado ou não, com ou sem internet, até mesmo se houve blackout na sua cidade.

Infelizmente, neste projeto, muitas vezes é necessário que você lide com os problemas sozinho. Por exemplo, cada corretora possui o MetaTrader de uma forma, e não é possível que seja ensinado de todas as corretoras. Como sempre é dito no Código.py, use a internet e o Google a seu favor, nunca teremos a resposta de tudo.

A primeira etapa do projeto é habilitar o MetaTrader 5 em sua corretora. Primeiramente, teste no MetaTrader 5 Simulado, pois ele simula o mercado igualmente, sendo que a única diferença é que você não está operando com dinheiro real. Após algum período de teste, com o MT5 funcionando corretamente sem nenhum risco de perder todo seu dinheiro com erro de programação, pode-se utilizar o MT5.

Portanto, ative o serviço e faça o download, mas pela sua própria corretora e não pelo Google, pois a corretora possui um serviço dentro do MT5 e tudo configurado, diferentemente se for feito pelo Google, em que você terá que realizar as devidas configurações.

Na AWS, crie uma EC2 com o sistema operacional do Windows, pois apenas com ele que o MT5 funciona. Utilize o par de chaves que já foi criado anteriormente, ou algum outro de sua preferência, assim como na configuração de rede, insira a VPC com a sub-rede conectada à internet, habilitando o IP público e edite o grupo de segurança que criamos, autorizando uma nova regra de entrada para “RDP”. Além disso, coloque um IP elástico, se você não lembra, foi feito no Projeto 1 - Dashboard Online, onde era fixado somente um único IP público.

Serviços Search [Alt+S]

Informações

Regras	Protocolo	Porta	Origem
sgr-0ea87e42763bd094e	TCP	3306	MySQL/Aurora
sgr-03277e5cabf8efc48	TCP	3306	MySQL/Aurora
sgr-0397245ae8b06a1a4	TCP	443	HTTPS
sgr-06a14c071e45ce7fd	TCP personalizado	8080	
sgr-038fa9b9646f09a7a	Todo o tráfego	Todo	Todo
sgr-0751877fdf3ed7125	TCP	22	SSH
sgr-08f00625a56cf1761	TCP	3306	MySQL/Aurora
sgr-001d42d39166c4e50	TCP	80	HTTP
-	TCP	3389	RDP

Adicionar regra

Conecte seu EC2:

EC2 > Instâncias > i-0a1ae48cf7c2910a3 > Conectar-se à instância

Conectar-se à instância

Conecte-se à sua instância i-0a1ae48cf7c2910a3 (algotradng-mt5) usando qualquer uma destas opções

Gerenciador de sessões **Cliente RDP** **Console de série do EC2**

Can't connect to your instance

To connect to an instance using Session Manager, Systems Manager requires an IAM instance profile. You can create an instance profile and assign it to your instance by using a Systems Manager Quick Setup [host management configuration](#). If you still can't connect to your instance, or if you receive an error, including an error about SSM Agent, see [Troubleshooting Session Manager](#).

[Open Systems Manager Quick Setup](#)

Uso do Gerenciador de sessões:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- As sessões são protegidas por uma chave do AWS Key Management Service.
- Você pode registrar comandos e detalhes de sessões em um bucket do Amazon S3 ou grupo de logs do CloudWatch Logs.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancelar **Conectar**

EC2 > Instâncias > i-0a1ae48cf7c2910a3 > Conectar-se à instância

Conectar-se à instância Informações

Conecte-se à sua instância i-0a1ae48cf7c2910a3 (algotradng-mt5) usando qualquer uma destas opções

Gerenciador de sessões | **Cliente RDP** | Console de série do EC2

ID de instância
 i-0a1ae48cf7c2910a3 (algotradng-mt5)

Tipo de conexão

Conecte-se usando o cliente RDP
Faça download de um arquivo para usar com seu cliente RDP e recupere sua senha.

Conecte-se usando o Fleet Manager
Para se conectar à instância usando o Desktop Remoto do Fleet Manager, o SSM Agent deve estar instalado e em execução na instância. Para obter mais informações, consulte [Trabalhar com o SSM Agent](#).

Você pode se conectar à sua instância do Windows usando uma área de trabalho remota cliente de sua preferência e fazendo o download e executando o arquivo de atalho de RDP abaixo:

Quando solicitado, conecte-se à sua instância usando os seguintes detalhes:

Public DNS
 ec2-3-87-244-42.compute-1.amazonaws.com

Nome do usuário
 Administrator

Senha

Se tiver ingresso sua instância em um diretório, você pode usar as credenciais do diretório para se conectar à sua instância.

Essa chave privada foi criada no mundo 10, quando estava sendo feita a criação da EC2, e essa chave não pode ser mostrada para absolutamente ninguém!

Obter senha do Windows Informações

Use sua chave privada para recuperar e descriptografar a senha inicial do administrador do Windows para essa instância.

ID de instância
 i-0a1ae48cf7c2910a3 (algotradng-mt5)

Par de chaves associado a essa instância
 Curso codigopy

Chave privada
Carregue o arquivo da chave privada ou copie e cole o conteúdo no campo abaixo.

Conteúdo da chave privada: *opcional*

Conteúdo da chave privada

Clique para copiar

Após descriptografar a senha, retorne na criação da instância em “Cliente RDP”, copie senha gerada e faça o download do arquivo de área de trabalho remota.

Conectar-se à instância [Informações](#)

Conecte-se à sua instância i-0a1ae48cf7c2910a3 (algotradng-mt5) usando qualquer uma destas opções

Gerenciador de sessões | **Cliente RDP** | Console de série do EC2

ID de instância
i-0a1ae48cf7c2910a3 (algotradng-mt5)

Tipo de conexão
 Conecte-se usando o cliente RDP
 Faça download de um arquivo para usar com seu cliente RDP e recupere sua senha.
 Conecte-se usando o Fleet Manager
 Para se conectar à instância usando o Desktop Remoto do Fleet Manager, o SSM Agent deve estar instalado e em execução na instância. Para obter mais informações, consulte [Trabalhar com o SSM Agent](#).

Você pode se conectar à sua instância do Windows usando uma área de trabalho remota cliente de sua preferência e fazendo o download e executando o arquivo de atalho de RDP abaixo:

Fazer download do arquivo de área de trabalho remota

Quando solicitado, conecte-se à sua instância usando os seguintes detalhes:

Public DNS
ec2-3-87-244-42.compute-1.amazonaws.com

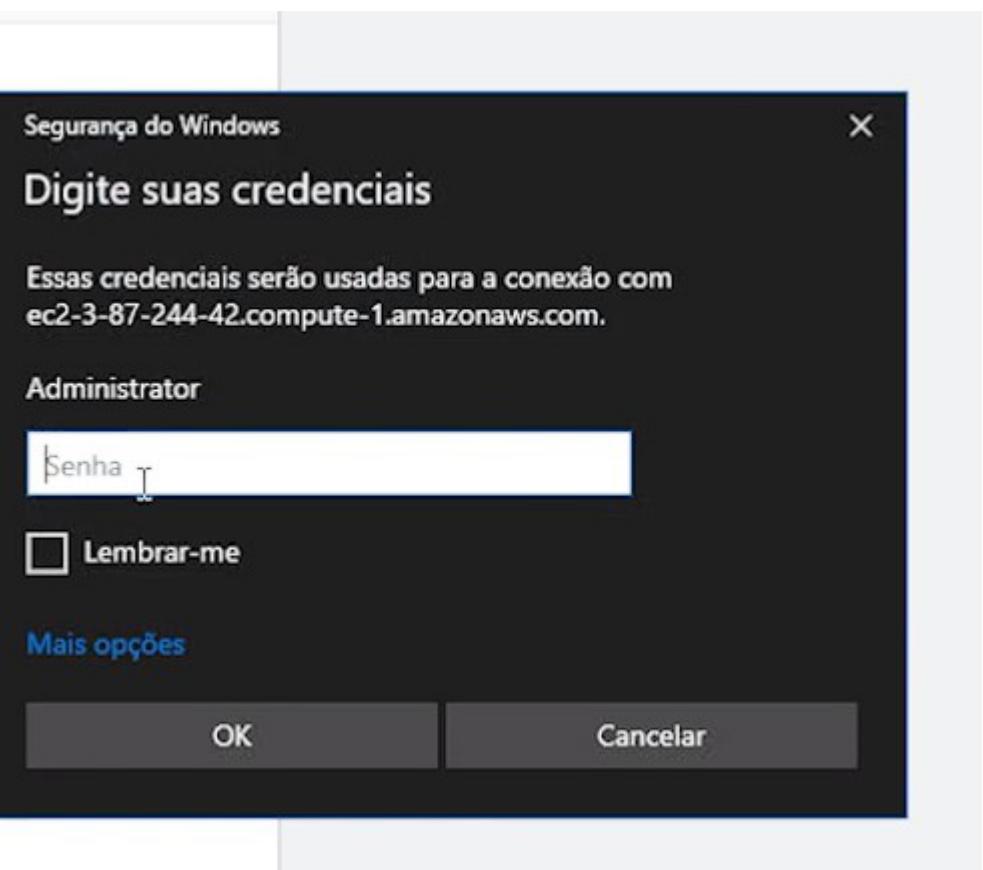
Nome do usuário
 Administrator

Senha
 jK9X096?qBhjOsGOTKLrZheXJlyU4ny

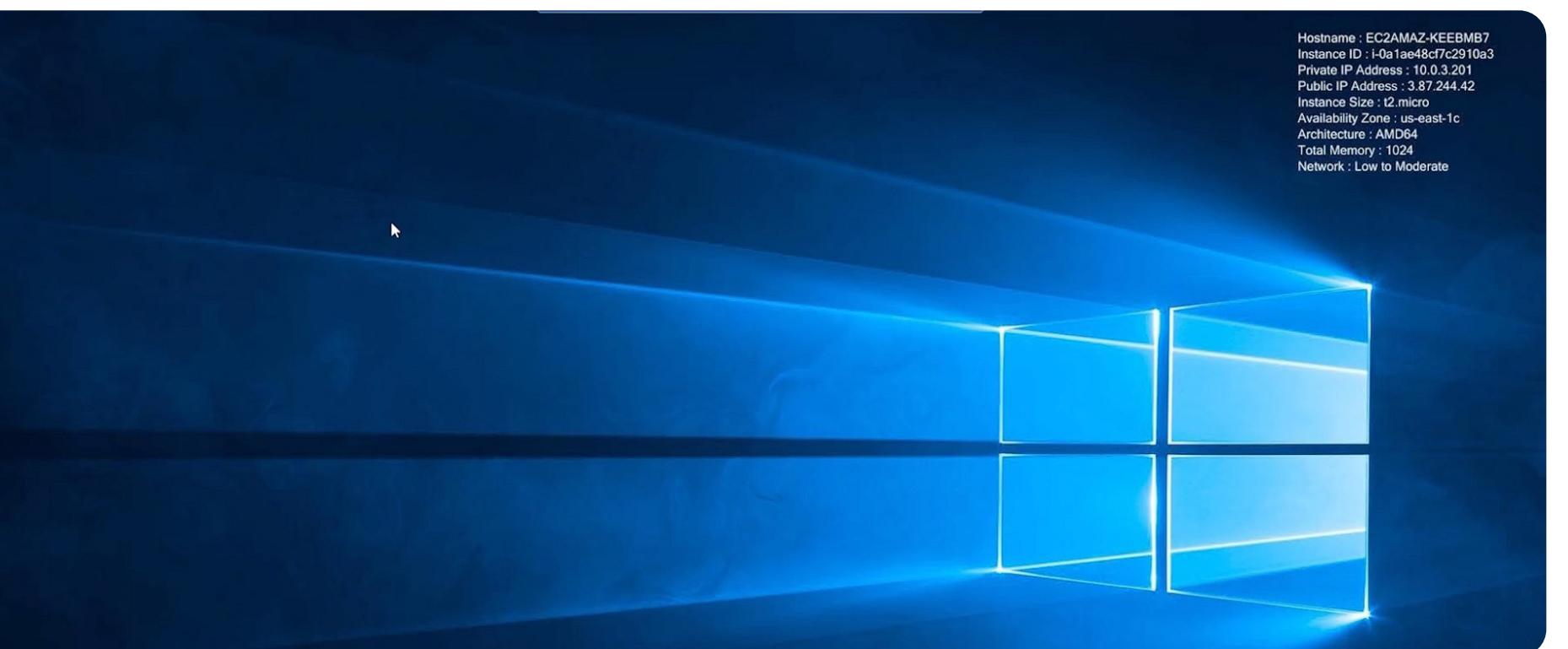
Se tiver ingresso sua instância em um diretório, você pode usar as credenciais do diretório para se conectar à sua instância.

[Cancelar](#)

Será solicitada a senha que você acabou de copiar.



Pronto, você tem um Windows rodando na sua AWS.



A partir deste momento, todas as etapas serão triviais e repetitivas. Como se fosse no computador da sua casa, é necessário baixar o Anaconda com o Python, VSCode, Git, MT5, etc. Porém, como esse computador é free-tier, provavelmente é mais lento que o computador da sua casa. Sempre faça todo o projeto no seu computador pessoal e só no final jogue pra nuvem através do GitHub.

No MT5, faça o login com sua corretora, e caso o “Algotrading” esteja verde, sua conta foi configurada corretamente.



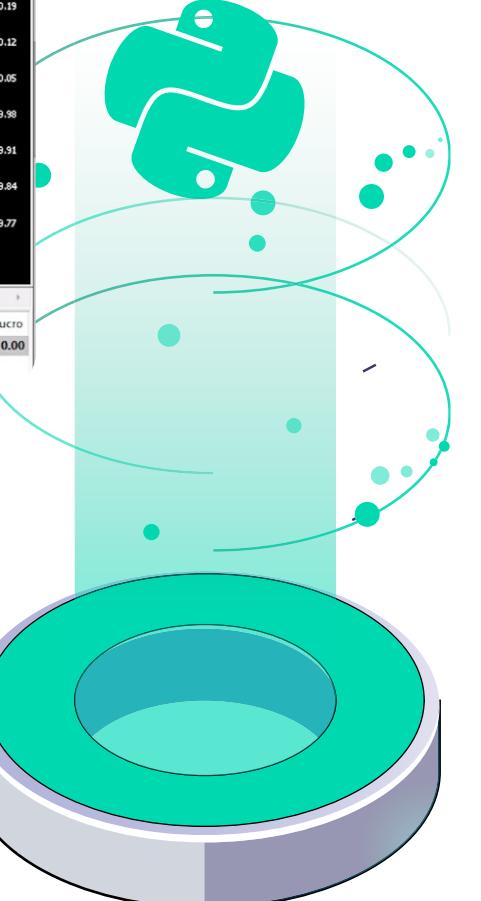
Quando o projeto estiver rodando em seu PC perfeitamente, jogue no EC2.

O MT5 tem uma documentação completa em português para integração com o Python. https://www.mql5.com/pt/docs/python_metatrader5.

O modelo que será implementado neste projeto, é o Bollinger Bands (ou Bandas de Bollinger) que foi utilizado no Mundo 10/11 da Galáxia 12 - Modelos de Análise Técnica. Portanto, pularemos a explicação acerca do código e seu funcionamento.

Após subir o projeto em seu computador, upo-o no GitHub, abra o Gtibash, e dê os comandos padrões:

```
git init
git add .
git commit -m "algotrading"
```



```

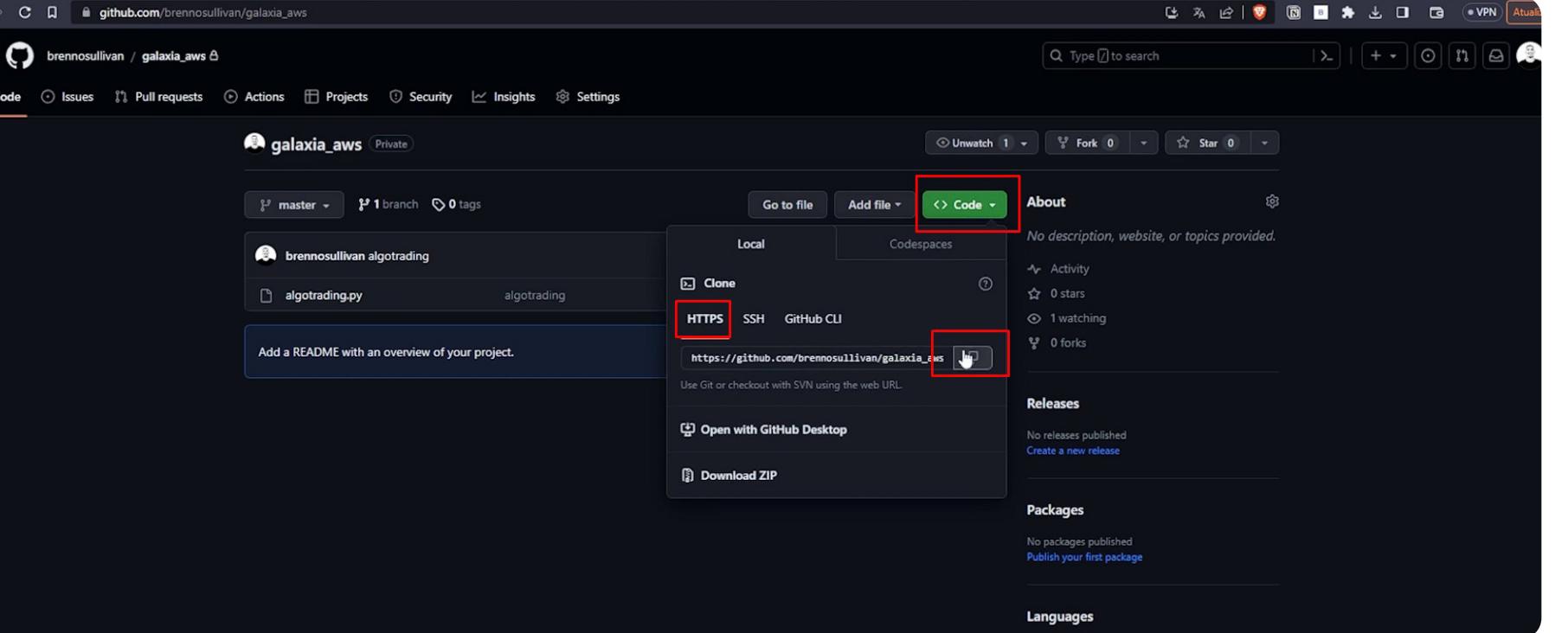
  SOURCE CONTROL  ⌂ ⌂ ⌂ ...
  algotrading.py x
  Message (Ctrl+Enter to commit ...)
  algotrading.py > git trading > ⌂ pega_dados_das_cotacoes_por_minuto() Publish to GitHub private repository brennosullivan/galaxia_aws
  type: ordem_mt5
  "type": "ordem_mt5",
  "price": ticker_info.buy
  "magic": 1,
  "comment": "Trades automaticos",
  "type_time": mt5.ORDER_TIME_DAY,
  "type_filling": mt5.ORDER_FILLING_RETURN,
  )
  result_compra = mt5.order_send(ordem_compra)
  print(result_compra)
  else:
    print("Nao foi possivel enviar a ordem para o ticker: " + ticker)

  def pegar_dados_das_cotacoes_por_minuto(self, ticker, intervalo, data_inicio, data_fim): #data de inicio e fim da leitura de dados
    dados = mt5.copy_rates_range(ticker, intervalo, data_inicio, data_fim)
    df_dados = pd.DataFrame(dados)
    df_dados['time'] = pd.to_datetime(df_dados['time'], unit='s')
    df_dados['time'] = df_dados['time'].dt.strftime('%Y-%m-%d %H:%M:%S')

    return df_dados

  if __name__ == "__main__":
    inicio = trading()
    ticker = 'PETR4'
    intervalo = mt5.TIMEFRAME_M1 #Existe uma lista de dataframes na documentacao
    data_fim = datetime.today()
    data_inicio = data_fim - timedelta(days=60)
    continuar = True
    while continuar == True:
      df_dados = inicio.pegar_dados_das_cotacoes_por_minuto(ticker, intervalo, data_inicio, data_fim)
      inicio.estategia_de_trade(df_data=df_dados, janela=50)

```



The screenshot shows the GitHub profile page for 'brennosullivan'. It lists repositories: 'galaxia_aws' (Private, Python, updated now), 'brennosullivan' (Public, Python, updated 4 hours ago), 'metatrader5' (Private, Python, updated yesterday), and 'dash-sample-apps' (Public, forked from plotly/dash-sample-apps, Open-source demos hosted on Dash Gallery, Jupyter Notebook, MIT License, updated yesterday).

Agora, entre na EC2, abra o VSCode, faça o login no GitHub, abra um novo terminal e mude para o Git Bash, e dê o comando para clonar o projeto, e depois abra a pasta que contenha o projeto.

`git clone https://github.com/brennosullivan/galaxia_aws`

```

File Edit Selection View Go Run Terminal Help
algotrading.py
algotrading.py
EXPLORER
GALAXIA_AWS
algotrading.py
import numpy as np
import pandas as pd
from datetime import datetime, timedelta
from time import sleep
import MetaTrader5 as mt5
import plotly.graph_objects as go
from plotly.subplots import make_subplots
|
class trading:
    def __init__(self) -> None:
        if not mt5.initialize():
            print("Deu problema ao inicializar o MetaTrader5")
        else:
            print("MetaTrader5 iniciado")
        self.posicao = [i._asdict() for i in mt5.positions_get()] #O que você tem comprado, sua posição naquela empresa
        self.ordens = [i._asdict() for i in mt5.orders_get()] #Ordens em aberto
        self.hist_ordens = [i._asdict() for i in mt5.history_orders_get(0, datetime.now())] #Histórico de ordens que foram abertas
        self.hist_ofertas = [i._asdict() for i in mt5.history_deals_get(0, datetime.now())] #Histórico de ofertas
    def estrategia_do_trade(self, janela, df_data):
        qtd_desvio = 1
        df_data["media"] = df_data["close"].rolling(janela).mean()
        df_data["desvio"] = df_data["close"].rolling(janela).std()
        df_data["media_alta"] = df_data["media"] + qtd_desvio * df_data["desvio"]
        df_data["media_baixa"] = df_data["media"] - qtd_desvio * df_data["desvio"]
        ultimo_preco = df_data["close"].iloc[-2]
        ultima_alta = df_data["media_alta"].iloc[-2]
        ultima_baixa = df_data["media_baixa"].iloc[-2]
|

```

Fazemos dessa forma pois o MT5 só funciona no Windows. Caso contrário, utilizáramos o Linux. O ideal é realizar tudo dentro do ambiente virtual como nos projetos anteriores, através do comando "requirements.txt".

Portanto, após essa etapa, a sua máquina EC2 pode ser fechada. Caso você se atente ao aviso, a AWS informará que o programa na sua EC2 continuará sendo executado mesmo desconectado.

```

File Edit Selection View Go Run Terminal Help
algotrading.py
algotrading.py
EXPLORER
GALAXIA_AWS
algotrading.py
ultima_preco = df_data["close"].iloc[-2]
ultima_alta = df_data["media_alta"].iloc[-2]
ultima_baixa = df_data["media_baixa"].iloc[-2]

print(f"Último Preço: {ultimo_preco} | Última Alta: {ultima_alta} | Última Baixa: {ultima_baixa}")

self.verificar_posicao_e_ordens()
if len(self.posicao) == 0:
    if ultimo_preco < ultima_baixa:
        self.enviar_ordens_para_mt5(ticker=ticker, ordem="buy", quantidade="100")
        print("Comprado")
    else:
        if ultimo_preco > ultima_alta:
            self.enviar_ordens_para_mt5(ticker=ticker, ordem="sell", quantidade="100")
            print("Vendido")
        else:
            print("Nenhuma ordem foi enviada")
    sleep(4)
def verificar_posicao_e_ordens(self):
    nova_posicao = [i._asdict() for i in mt5.positions_get()]
    nova_ordens = [i._asdict() for i in mt5.orders_get()]
    check = (self.posicao != nova_posicao) or (self.ordens != nova_ordens)
    self.posicao = nova_posicao
    self.ordens = nova_ordens
    return check
|

```

Portanto, o projeto foi finalizado e seu modelo de investimento está conectado à bolsa de valores, sendo 100% automatizado.