



Laboratório VPC

Objetivo: Criar uma VPC funcional com uma sub-rede pública e uma privada, configurar segurança básica e testar a conectividade.

Cenário: Você precisa criar uma rede virtual isolada na AWS para hospedar seus recursos. Essa rede terá uma sub-rede pública para um servidor web e uma sub-rede privada para um banco de dados, garantindo a segurança e o isolamento dos seus dados.

Pré-requisitos:

- Uma conta AWS com acesso ao console de gerenciamento.
- Navegador web.
- **MobaXterm (Portable Edition):**
https://download.mobatek.net/2502024121622306/MobaXterm_Portable_v25.0.zip

Tarefas:

1. Criar a VPC:

- **Passo 1:** Acesse o console AWS e selecione a Região AWS **us-east-1 (Norte da Virgínia)**.
- **Passo 2:** Acesse o console do VPC: Abra seu navegador web e acesse o console de gerenciamento da AWS. No menu de serviços, procure por "VPC" e clique nele.
- **Passo 3:** Clique em "Suas VPCs" e depois em "Criar VPC".
- **Passo 4:** Escolha a opção "**VPC e muito mais**".
- **Passo 5:** Em "**Geração automática da etiqueta de nome**", mude o nome "projeto" por "**MinhaVPC-seu-nome-sobrenome**".

Architected Solutions AWS

- **Passo 6:** Defina um bloco CIDR para sua VPC: **10.0.0.0/16**.
- **Passo 7:** Em "Tenancy = Locação ", selecione **"Default = padrão"**.
- **Passo 8:** Em "Número de zonas de disponibilidade (AZs)" escolha **1**.
- **Passo 9:** Em "Número de sub-redes públicas", escolha **1**.
- **Passo 10:** Em "Número de sub-redes privadas", escolha **1**.
- **Passo 11:** Em "Gateways NAT", selecione **"Nenhum"**.
- **Passo 12:** Em "Endpoints da VPC", selecione **"Nenhum"**.
- **Passo 13:** Clique em **"Personalizar blocos CIDR de sub-redes"**
- **Passo 14:** Em "Bloco CIDR da sub-rede pública em us-east-1a", informe **"10.0.1.0/24"**
- **Passo 15:** Em "Bloco CIDR da sub-rede privada em us-east-1a", informe **"10.0.20.0/24"**
- **Passo 16:** Finalize clicando em **"Criar VPC"**
- **Passo 17:** Verifique se a VPC foi criada clicando em "Suas VPCs".

<input type="checkbox"/>	Name	ID da VPC	Estado	Bloquear a...	CIDR IPv4	CIDR IPv6
<input type="checkbox"/>	MinhaVPCLab4-vpc	yvc-001e35e6543d9cd69	Available	Desativado	10.0.0.0/16	-
<input type="checkbox"/>	-	yvc-0db0ef7e822260233	Available	Desativado	172.31.0.0/16	-
<input type="checkbox"/>	MinhaVPC-Sidney-Richelle-vpc	yvc-0b297d948d09e236a	Available	Desativado	10.0.0.0/16	-
<input type="checkbox"/>	MinhaVPC-JoaoPaz-vpc	yvc-0ff245f3bb8d65621	Available	Desativado	10.0.0.0/16	-
<input type="checkbox"/>	MinhaVPC-Lucas-Albino-vpc	yvc-062baf1348b616f5b	Available	Desativado	10.0.0.0/16	-

Configurações da VPC

Recursos a serem criados **Informações**

Crie apenas o recurso da VPC ou a VPC e outros recursos de rede.

☐ Somente VPC ☒ VPC e muito mais

Geração automática da etiqueta de nome **Informações**

Insira um valor para a etiqueta de nome. Esse valor será usado para gerar automaticamente etiquetas de nome para todos os recursos na VPC.

☒ Gerar automaticamente

MinhaVPC-Sabrina

Bloco CIDR IPv4 **Informações**

Determine o IP inicial e o tamanho da VPC usando notação CIDR.

10.0.0.0/16 65.536 IPs

O tamanho do bloco CIDR deve estar entre /16 e /28.

Bloco CIDR IPv6 **Informações**

☒ Nenhum bloco CIDR IPv6

☐ Bloco CIDR IPv6 fornecido pela Amazon

Previsualização

VPC **Mostrar detalhes**

Sua rede virtual da AWS

MinhaVPC-Sabrina-vpc

Sub-redes (4)

Sub-redes dentro dessa VPC

us-east-1a

- MinhaVPC-Sabrina-subnet-public1
- MinhaVPC-Sabrina-subnet-private1

us-east-1b

- MinhaVPC-Sabrina-subnet-public2
- MinhaVPC-Sabrina-subnet-private2

Tabelas de rotas

Rotear o tráfego de rede

- MinhaVPC-Sabrina-rt
- MinhaVPC-Sabrina-rt
- MinhaVPC-Sabrina-rt

Architected Solutions AWS

[Alt+S]

Estados Unidos (Norte da Virginia)

sabrina.dev@outlook.com @ 1608-8526-6406

VPC > Suas VPCs > Criar VPC

Número de zonas de disponibilidade (AZs) [Informações](#)
Escolha o número de AZs em que as sub-redes deverão ser provisionadas. Para alta disponibilidade, recomendamos pelo menos duas AZs.

1

2

3

► Personalizar AZs

Número de sub-redes públicas [Informações](#)
O número de sub-redes públicas a serem adicionadas à sua VPC. Use sub-redes públicas para aplicações Web que precisam estar publicamente acessíveis pela Internet.

0

1

Número de sub-redes privadas [Informações](#)
O número de sub-redes privadas a serem adicionadas à sua VPC. Use sub-redes privadas para proteger recursos de backend que não precisam de acesso público.

0

1

2

► Personalizar blocos CIDR de sub-redes

Gateways NAT (USD) [Informações](#)
Escolha o número de zonas de disponibilidade (AZs) nas quais criar gateways NAT. Observe que há uma cobrança para cada gateway NAT.

Nenhuma

Em 1 AZ

1 por AZ

Localização

Você pode executar instâncias em sua VPC em hardware dedicado de locatário único.

Selecione **Padrão** para garantir que as instâncias executadas nessa VPC usem o atributo de localização especificado na execução ou se você estiver criando uma VPC para conectividade privada do Outposts.

Selecione **Dedicada** para garantir que as instâncias executadas nesta VPC sejam executadas em instâncias de localização dedicadas, independentemente do atributo de localização especificado na execução.

Se suas VPCs do Outposts exigirem conectividade privada, você deverá selecionar **Padrão**.

Saiba mais ⓘ
Criando uma VPC

VPC > Suas VPCs > Criar VPC

012

► Personalizar blocos CIDR de sub-redes

Gateways NAT (USD) [Informações](#)

Escolha o número de zonas de disponibilidade (AZs) nas quais criar gateways NAT. Observe que há uma cobrança para cada gateway NAT.

Nenhuma

Em 1 AZ

1 por AZ

Endpoints da VPC [Informações](#)

Os endpoints podem ajudar a reduzir as cobranças do gateway NAT e melhorar a segurança acessando o S3 diretamente da VPC. Por padrão, a política de acesso integral será usada. Você pode personalizar essa política a qualquer momento.

Nenhuma

Gateway do S3


Opções de DNS [Informações](#)

☒ Habilitar nomes de host DNS

☒ Habilitar resolução de DNS

► Tags adicionais

Cancelar

 Código de visualização

Criar VPC

1


Localização

Você pode executar instâncias em sua VPC em hardware dedicado de locatário único.

Selecione **Padrão** para garantir que as instâncias executadas nessa VPC usem o atributo de localização especificado na execução ou se você estiver criando uma VPC para conectividade privada do Outposts.

Selecione **Dedicada** para garantir que as instâncias executadas nesta VPC sejam executadas em instâncias de localização dedicadas, independentemente do atributo de localização especificado na execução.

Se suas VPCs do Outposts exigirem conectividade privada, você deverá selecionar **Padrão**.





Saiba mais 

[Criando uma VPC](#)

aws

Q Search

[Alt+S]



Estados Unidos (Norte da Virgínia)

sabrina.idev@outlook.com @ 1608-8526-6406

VPC > Suas VPCs > Criar VPC

O número de sub-redes públicas a serem adicionadas à sua VPC. Use sub-redes públicas para aplicações Web que precisam estar publicamente acessíveis pela Internet.

01

Número de sub-redes privadas [Informações](#)

O número de sub-redes privadas a serem adicionadas à sua VPC. Use sub-redes privadas para proteger recursos de backend que não precisam de acesso público.

012

▼ Personalizar blocos CIDR de sub-redes

Bloco CIDR da sub-rede pública em us-east-1a

10.0.1.0/24256 IPs

Bloco CIDR da sub-rede privada em us-east-1a

10.0.20.0/24256 IPs

<>^v

Gateways NAT (USD) [Informações](#)

Escolha o número de zonas de disponibilidade (AZs) nas quais criar gateways NAT. Observe que há uma cobrança para cada gateway NAT.

NenhumaEm 1 AZ1 por AZ

Endpoints da VPC [Informações](#)

Architected Solutions AWS

VPC > Suas VPCs > Criar VPC > Criar recursos da VPC

Criar fluxo de trabalho de VPC

Erro

Detalhes

Criar VPC

The maximum number of VPCs has been reached.

Cancelar

Voltar

Tentar novamente

aws Search [Alt+S] Estados Unidos (Ohio) sabrina.iddev@outlook.com @ 1608-8526-6406

VPC > Suas VPCs > Criar VPC

Número de sub-redes privadas [Informações](#)

O número de sub-redes privadas a serem adicionadas à sua VPC. Use sub-redes privadas para proteger recursos de backend que não precisam de acesso público.

0 1 2

Personalizar blocos CIDR de sub-redes

Bloco CIDR da sub-rede pública em us-east-2a

10.0.0.0/20 4.096 IPs

Bloco CIDR da sub-rede privada em us-east-2a

10.0.128.0/20 4.096 IPs

Gateways NAT (USD) [Informações](#)

Escolha o número de zonas de disponibilidade (AZs) nas quais criar gateways NAT. Observe que há uma cobrança para cada gateway NAT.

Nenhuma Em 1 AZ 1 por AZ

Endpoints da VPC [Informações](#)

Os endpoints podem ajudar a reduzir as cobranças do gateway NAT e melhorar a segurança acessando o S3 diretamente da VPC. Por padrão, a política de acesso integral será usada. Você pode personalizar essa política a qualquer momento.

Nenhuma Gateway do S3

aws Search [Alt+S] Estados Unidos (Ohio) sabrina.iddev@outlook.com @ 1608-8526-6406

VPC > Suas VPCs > Criar VPC > Criar recursos da VPC

Criar fluxo de trabalho de VPC

Verificando criação da tabela de rotas 93%

Detalhes

- ✓ Criar VPC: vpc-07e006789db8ee117
- ✓ Habilitar nomes de host DNS
- ✓ Habilitar resolução de DNS
- ✓ Verificando a criação da VPC: vpc-07e006789db8ee117
- ✓ Criar sub-rede: subnet-08203780782bc978e
- ✓ Criar sub-rede: subnet-075fd40c5b4cf4624
- ✓ Criar gateway da Internet: igw-0c785474745f595eb
- ✓ Anexar gateway da Internet à VPC
- ✓ Criar tabela de rotas: rtb-006636404587f310e
- ✓ Criar rota
- ✓ Associar tabela de rotas
- ✓ Criar tabela de rotas: rtb-082f003d7cf50d3a2
- ✓ Associar tabela de rotas
- Verificando criação da tabela de rotas

CloudShell Comentários © 2025, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

2. Criar Grupos de Segurança:

- **Passo 1:** No painel de navegação, clique em "Grupos de segurança" e depois em "Criar grupo de segurança".
- **Passo 2:** Informe um nome para o grupo de segurança: **"SG-Web-seu-nome-sobrenome"**.
- **Passo 3:** Em "Descrição", adicione: **"Regras para acesso ao servidor web"**.
- **Passo 4:** Selecione a VPC que você criou (**MinhaVPC-seu-nome-sobrenome**).
- **Passo 5:** Na seção "Regras de entrada", clique em "Adicionar regra".
- **Passo 6:** Em "Tipo", selecione **"HTTP"**.
- **Passo 7:** Em "Origem", selecione **"Qualquer local-IPv4" (0.0.0.0/0)**.
- **Passo 8:** Clique novamente em "Adicionar regra".

- **Passo 9:** Em "Tipo", selecione **"HTTPS"**.
- **Passo 10:** Em "Origem", selecione **"Qualquer local-IPv4" (0.0.0.0/0)**.
- **Passo 11:** Clique novamente em "Adicionar regra".
- **Passo 12:** Em "Tipo", selecione **"SSH"**.
- **Passo 13:** Em "Origem", selecione **"Meu IP"**.
- **Passo 14:** Clique em "Criar grupo de segurança".
- **Passo 15:** Repita os passos 1 a 4 para criar um grupo de segurança para a instância de banco de dados:
 - Nome: **"SG-BD-seu-nome-sobrenome"**
 - Descrição: **"Regras para acesso ao servidor de banco de dados"**
- **Passo 16:** No grupo de segurança do banco de dados (**SG-BD-seu-nome-sobrenome**), adicione as seguintes regras de entrada:
 - **Passo 16.1:** Clique em "Adicionar regra".
 - **Passo 16.2:** Em "Tipo", selecione **"SSH"**.
 - **Passo 16.3:** Em "Origem", selecione **"Personalizado"** e, no campo ao lado, insira o bloco CIDR da sua VPC: **10.0.0.0/16**.
 - **Passo 16.4 (MySQL):** Clique em "Adicionar regra".
 - Em "Tipo", selecione **"MySQL/Aurora"**.
 - Em "Origem", selecione **"Personalizado"** e, no campo ao lado, insira o bloco CIDR da sua VPC: **10.0.0.0/16**.
 -
 - **Passo 16.5 (PostgreSQL - Opcional):** Se for usar PostgreSQL, clique em "Adicionar regra".
 - Em "Tipo", selecione **"PostgreSQL"**.
 - Em "Origem", selecione **"Personalizado"** e, no campo ao lado, insira o bloco CIDR da sua VPC: **10.0.0.0/16**.
- **Passo 17:** Clique em "Criar grupo de segurança".

VPC > Grupos de segurança > Criar grupo de segurança

Criar grupo de segurança Informações

Um grupo de segurança atua como um firewall virtual para sua instância para controlar o tráfego de entrada e saída. Para criar um novo grupo de segurança, preencha os campos abaixo.

Detalhes básicos

Nome do grupo de segurança Informações

SG-Web- Sabrina

O nome não pode ser editado após a criação.

Descrição Informações

Regras para acesso ao servidor web

VPC Informações

vpc-07e006789db8ee117 (MinhaVPC-Sabrina-vpc) ▼

Regras de entrada Informações

Este grupo de segurança não tem regras de entrada.

[Adicionar regra](#)

Architected Solutions AWS

aws

Search

[Alt+S]

Estados Unidos (Ohio)

sabrina.iddev@outlook.com @ 1608-8526-6406

VPC

Grupos de segurança

Criar grupo de segurança

Regras de entrada

Informações

Tipo

Informações

Protocolo

Informações

Intervalo de portas

Informações

Origem

Informações

Descrição - opcional

Informações

HTTP

TCP

80

Qualq...

0.0.0.0/0

Excluir

HTTPS

TCP

443

Qualq...

0.0.0.0/0

Excluir

SSH

TCP

22

Meu IP

191.57.26.54/32

Excluir

Adicionar regra

As regras com a origem 0.0.0.0/0 ou ::/0 permitem que todos os endereços IP acessem a instância. Recomendamos configurar as regras de grupo de segurança para permitir o acesso apenas de endereços IP conhecidos.

Regras de saída

Informações

aws

Search

[Alt+S]

Estados Unidos (Ohio)

sabrina.iddev@outlook.com @ 1608-8526-6406

VPC

Grupos de segurança

sg-06065538de4e5d95a - SG-Web- Sabrina

Painel da VPC

Visualização global do EC2

Filtrar por VPC

Nuvem privada virtual

Suas VPCs

Sub-redes

Tabelas de rotas

Gateways da Internet

Gateways da Internet somente de saída

Conjuntos de opções de DHCP

IPs elásticos

Listas de prefixos gerenciados

Gateways NAT

Conexões de emparelhamento

Segurança

O grupo de segurança (sg-06065538de4e5d95a | SG-Web- Sabrina) foi criado com êxito

Detalhes

sg-06065538de4e5d95a - SG-Web- Sabrina

Ações

Detalhes

Nome do grupo de segurança

sg-Web- Sabrina

ID do grupo de segurança

sg-06065538de4e5d95a

Descrição

Regras para acesso ao servidor web

ID da VPC

vpc-07e006789db8ee117

Proprietário

160885266406

Número de regras de entrada

3 Entradas de permissão

Número de regras de saída

1 Entrada de permissão

Regras de entrada

Regras de saída

Compartilhamento - novo

Associações da VPC - novo

Tags

Regras de entrada (3)

Gerenciar tags

Editar regras de entrada

Pesquisar

Name

ID da regra do grup...

Versão do IP

Tipo

Protocolo

Intervalo de portas

SSH

TCP

??

aws

Search

[Alt+S]

Estados Unidos (Ohio)

sabrina.iddev@outlook.com @ 1608-8526-6406

VPC

Grupos de segurança

Criar grupo de segurança

Criar grupo de segurança

Informações

Um grupo de segurança atua como um firewall virtual para sua instância para controlar o tráfego de entrada e saída. Para criar um novo grupo de segurança, preencha os campos abaixo.

Detalhes básicos

Nome do grupo de segurança

Informações

SG-BD-SabrinaRodrigues

O nome não pode ser editado após a criação.

Descrição

Informações

Regras para acesso ao servidor de banco de dados

VPC

Informações

vpc-07e006789db8ee117 (MinhaVPC-Sabrina-vpc)

Regras de entrada

Informações

Este grupo de segurança não tem regras de entrada.

Adicionar regra

Architected Solutions AWS

The first screenshot shows the 'Criar grupo de segurança' (Create security group) page in the AWS console. It displays the 'Regras de entrada' (Inbound rules) section with three rules: SSH (TCP, port 22), MySQL/Aurora (TCP, port 3306), and PostgreSQL (TCP, port 5432). Each rule is associated with the 'vpc-07e006789db8ee117' VPC. The 'Origem' (Source) for all rules is set to '10.0.0.0/16'. The 'Descrição - opcional' (Optional description) field is empty for all rules. The 'Adicionar regra' (Add rule) button is visible at the bottom left.

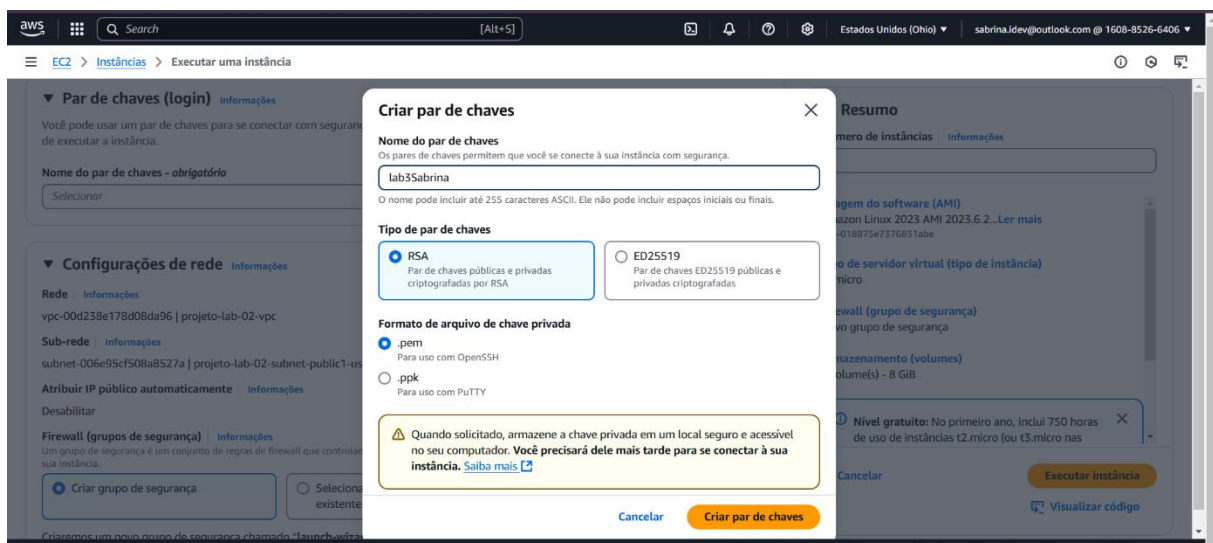
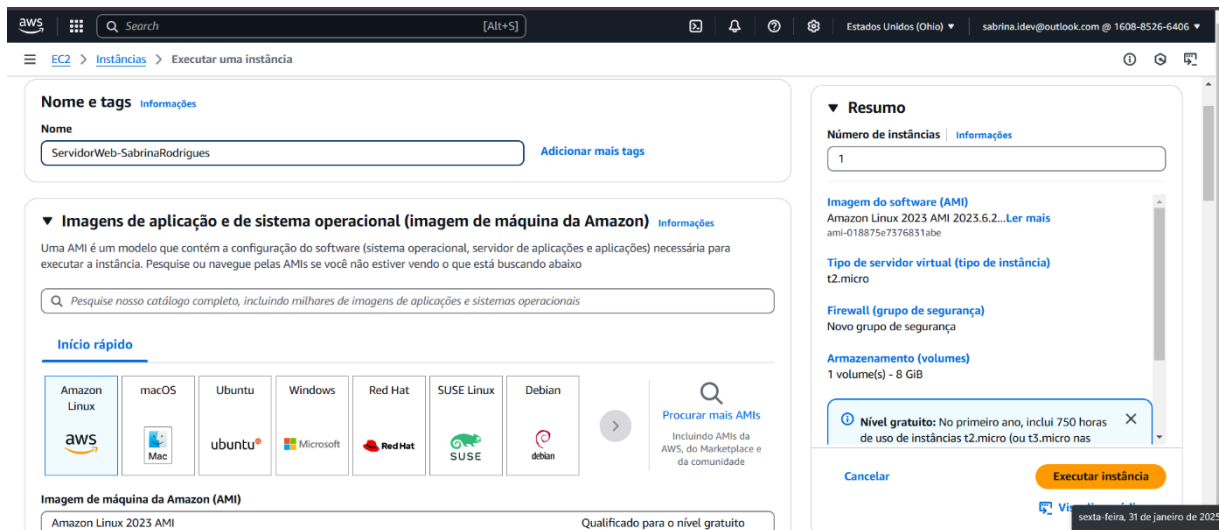
The second screenshot shows the 'Painel da VPC' (VPC Dashboard) for the 'sg-0ee1d0bdc7b108a' security group. A green notification banner at the top states: 'O grupo de segurança (sg-0ee1d0bdc7b108a | SG-BD-SabrinaRodrigues) foi criado com êxito' (The security group was created successfully). The 'Detalhes' (Details) section shows the group name 'SG-BD-SabrinaRodrigues', ID 'sg-0ee1d0bdc7b108a', owner '160885266406', and 3 inbound rules. The 'Regras de entrada' (Inbound rules) tab is selected, showing a list of 3 rules. The 'Gerenciar tags' (Manage tags) and 'Editar regras de entrada' (Edit inbound rules) buttons are visible at the top right of the rules list.

3. Lançar Instâncias EC2:

- **Passo 1:** No menu de serviços, procure por "EC2" e clique nele.
- **Passo 2:** Clique em "Instâncias" e depois em "Executar instâncias".
- **Passo 3:** Em "Nome", informe: **ServidorWeb-seu-nome-sobrenome**.
- **Passo 4:** Em "Imagem da Amazon Machine (AMI)", selecione: **Amazon Linux 2023 (HVM), SSD Volume Type**.
- **Passo 5:** Em "Tipo de instância", escolha: **t2.micro**.
- **Passo 6:** Em "Par de chaves (login)", crie um novo par de chaves ou use um existente.
 - Se for criar um novo, clique em "**Criar novo par de chaves**".
 - Nome do par de chaves: **SeuNome**.
 - Tipo de Chave Privada: **.pem**
 - Clique em "**Criar par de chaves**".
 - **Salve o arquivo SeuNome.pem em um local seguro.**
- **Passo 7:** Em "Configurações de rede", clique em "Editar".
- **Passo 8:** Em "VPC - Obrigatório", selecione a VPC que você criou (**MinhaVPC-seu-nome-sobrenome**).
- **Passo 9:** Em "Sub-rede", selecione a **sub-rede pública (10.0.1.0/24)**.
- **Passo 10:** Em "Atribuir automaticamente IP público", verifique se está **Habilitado**.
- **Passo 11:** Em "Grupo de segurança", escolha "**Selecionar grupo de segurança existente**".
- **Passo 12:** Em "Grupos de segurança comuns", escolha "**SG-Web-seu-nome-sobrenome**".

Architected Solutions AWS

- **Passo 13:** Em "**Configurações de armazenamento**", deixe como padrão.
- **Passo 14:** Clique em "**Executar instância**".
- **Passo 15:** Repita os passos 2 a 6 e 13 e 14 para lançar a instância **ServidorBD-seu-nome-sobrenome**. Os demais passos serão detalhados abaixo.
 - **Passo 15.1:** Em "Nome", informe: **ServidorBD-seu-nome-sobrenome**.
 - **Passo 15.2:** Em "**Configurações de rede**", clique em "**Editar**".
 - **Passo 15.3:** Em "VPC - *Obrigatório*", selecione a VPC que você criou (**MinhaVPC-seu-nome-sobrenome**).
 - **Passo 15.4:** Em "Sub-rede", selecione a **sub-rede privada (10.0.20.0/24)**.
 - **Passo 15.5:** Em "Atribuir automaticamente IP público", certifique-se de que esteja **Desabilitado**.
 - **Passo 15.6:** Em "Grupo de segurança", escolha "**Selecionar grupo de segurança existente**".
 - **Passo 15.7:** Em "**Grupos de segurança comuns**", escolha "**SG-BD-seu-nome-sobrenome**".
 - **Passo 15.8:** Em "Tipo de instância", escolha: **t2.micro**.
 - **Passo 15.9:** Em "Par de chaves (login)", selecione **Lab4** (ou o nome que você deu ao par de chaves).



Architected Solutions AWS

EC2 > Instâncias > Executar uma instância

VPC - obrigatório

Informações

vpc-07e006789db8ee117 (MinhaVPC-Sabrina-vpc)

10.0.0.0/16

Sub-rede

Informações

subnet-08203780782bc978e

MinhaVPC-Sabrina-subnet-public1-us-east-2a

VPC: vpc-07e006789db8ee117 Proprietário: 160885266406

Zona de disponibilidade: us-east-2a Tipo de zona: Zona de disponibilidade

Endereços IP disponíveis: 4091 CIDR: 10.0.0.0/20

Atribuir IP público automaticamente

Informações

Habilitar

Taxas adicionais se aplicam quando fora do limite de nível gratuito

Firewall (grupos de segurança)

Informações

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

☐ Criar grupo de segurança

☒ Selecionar grupo de segurança existente

Grupos de segurança comuns

Informações

Selecionar grupos de segurança

SG-Web- Sabrina sg-06065538de4e5d95a

VPC: vpc-07e006789db8ee117

Comparar regras do grupo de segurança

Os grupos de segurança que você adicionar ou remover aqui serão adicionados ou removidos em todas as suas interfaces de rede.

Resumo

Número de instâncias

Informações

1

Imagem do software (AMI)

Amazon Linux 2023 AMI 2023.6.2...[Ler mais](#)

ami-018875e7376831abe

Tipo de servidor virtual (tipo de instância)

t2.micro

Firewall (grupo de segurança)

SG-Web- Sabrina

Armazenamento (volumes)

1 volume(s) - 8 GiB

Nível gratuito: No primeiro ano, inclui 750 horas de uso de instâncias t2.micro (ou t3.micro nas

Cancelar

Executar instância

[Visualizar código](#)

EC2 > Instâncias > Executar uma instância

Executar uma instância

Informações

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

Nome e tags

Informações

Nome

ServidorBD-SabrinaRodrigues

[Adicionar mais tags](#)

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

Informações

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

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

Recentes

Início rápido

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

[Procurar mais AMIs](#)

Incluindo AMIs da AWS, do Marketplace e

Resumo

Número de instâncias

Informações

1

t2.micro

Firewall (grupo de segurança)

Novo grupo de segurança

Armazenamento (volumes)

1 volume(s) - 8 GiB

Nível gratuito: No primeiro ano, inclui 750 horas de uso de instâncias t2.micro (ou t3.micro nas regiões em que o t2.micro está indisponível) em AMIs de nível gratuito por mês, 750 horas de uso de endereço IPv4 público por mês, 30 GiB de armazenamento do EBS, 2 milhões de E/S, 1 GB de snapshots e 100 GB de largura de banda para

Cancelar

Executar instância

[Visualizar código](#)

EC2 > Instâncias > Executar uma instância

Nome do par de chaves - obrigatório

lab3Sabrina

[Criar novo par de chaves](#)

Configurações de rede

Informações

VPC - obrigatório

Informações

vpc-07e006789db8ee117 (MinhaVPC-Sabrina-vpc)

10.0.0.0/16

Sub-rede

Informações

subnet-075fd40c5b4cf4624

MinhaVPC-Sabrina-subnet-private1-us-east-2a

VPC: vpc-07e006789db8ee117 Proprietário: 160885266406

Zona de disponibilidade: us-east-2a Tipo de zona: Zona de disponibilidade

Endereços IP disponíveis: 4091 CIDR: 10.0.128.0/20

Atribuir IP público automaticamente

Informações

Desabilitar

Firewall (grupos de segurança)

Informações

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

☒ Criar grupo de segurança

☐ Selecionar grupo de segurança existente

Nome do grupo de segurança - obrigatório

Resumo

Número de instâncias

Informações

1

t2.micro

Firewall (grupo de segurança)

Novo grupo de segurança

Armazenamento (volumes)

1 volume(s) - 8 GiB

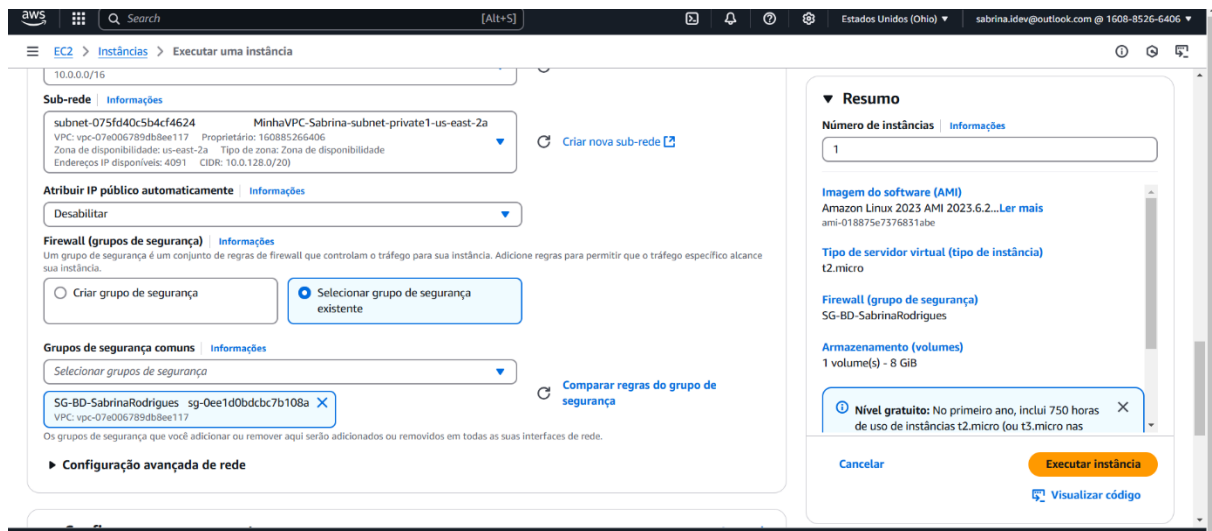
Nível gratuito: No primeiro ano, inclui 750 horas de uso de instâncias t2.micro (ou t3.micro nas regiões em que o t2.micro está indisponível) em AMIs de nível gratuito por mês, 750 horas de uso de endereço IPv4 público por mês, 30 GiB de armazenamento do EBS, 2 milhões de E/S, 1 GB de snapshots e 100 GB de largura de banda para

Cancelar

Executar instância

[Visualizar código](#)

Architected Solutions AWS



4. Testar a Conectividade (Usando MobaXterm):

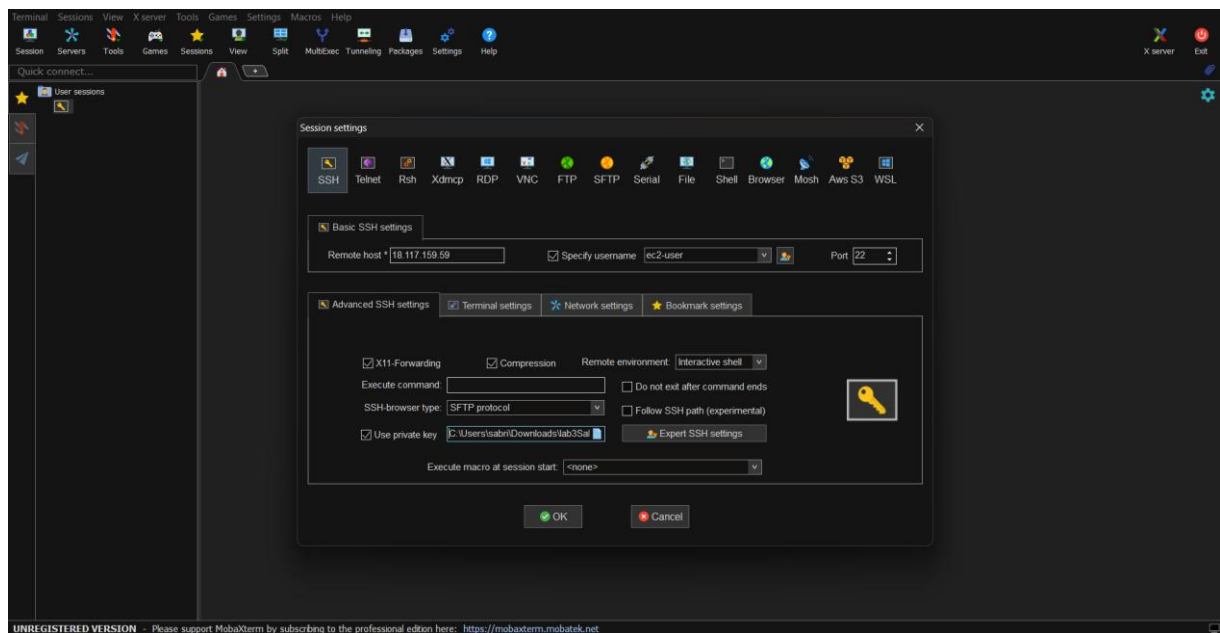
- **Passo 1:** Baixe e instale o MobaXterm
 - Baixe o MobaXterm Portable Edition:
https://download.mobatek.net/2502024121622306/MobaXterm_Portable_v25.0.zip
 - Extraia o conteúdo do arquivo zip para uma pasta de sua preferência.
 - Execute o arquivo MobaXterm_Personal_25.0.exe
- **Passo 2:** Conecte-se à instância web (**ServidorWeb-seu-nome-sobrenome**) via SSH usando o MobaXterm.
 - No MobaXterm, clique em **"Session"** e selecione **"SSH"**.
 - Em **"Remote host"**, insira o endereço IP público do **ServidorWeb-seu-nome-sobrenome** (você encontra esse IP no console da AWS, na descrição da instância).
 - Marque **"Specify username"** e insira: ec2-user.
 - Clique em **"Advanced SSH settings"**.
 - Marque **"Use private key"** e selecione o arquivo **.pem** que você baixou (ex: **SeuNome.pem**).
 - Clique em **"OK"**.
 - Se for solicitado a confirmar a chave, clique em **"Accept"**.
- **Passo 3:** A partir da instância web (**ServidorWeb-seu-nome-sobrenome**), tente acessar a internet. Utilize o comando ping 8.8.8.8. Deve funcionar. **(TIRE UM PRINT DESSA TELA PARA ANEXAR NA ATIVIDADE AO FINALIZAR NO CLASSROOM)**
- **Passo 4:** Conecte-se à instância do banco de dados (**ServidorBD-seu-nome-sobrenome**) via SSH, utilizando a instância web (**ServidorWeb-seu-nome-sobrenome**) como "trampolim" (bastion host).
- ****A partir da sessão SSH já aberta para o ServidorWeb-seu-nome-sobrenome no MobaXterm, ****faça o seguinte procedimento: `ssh -i "<caminho_para_chave>/SeuNome.pem" ec2-user@<endereço_IP_privado_do_ServidorBD-seu-nome-sobrenome>` (Substitua <caminho_para_chave> pelo caminho onde você salvou o arquivo **SeuNome.pem** e <endereço_IP_privado_do_ServidorBD-seu-nome-sobrenome> pelo IP privado do **ServidorBD-seu-nome-sobrenome** - você

- **Passo 5:** A partir da instância do banco de dados (**ServidorBD-seu-nome-sobrenome**), tente acessar a internet. O comando ping 8.8.8.8 **não deve funcionar**, pois a instância está em uma sub-rede privada sem acesso à internet pois o NAT Gateway não foi configurado na criação da VPC. **(TIRE UM PRINT DESSA TELA PARA ANEXAR NA ATIVIDADE AO FINALIZAR NO CLASSROOM)**

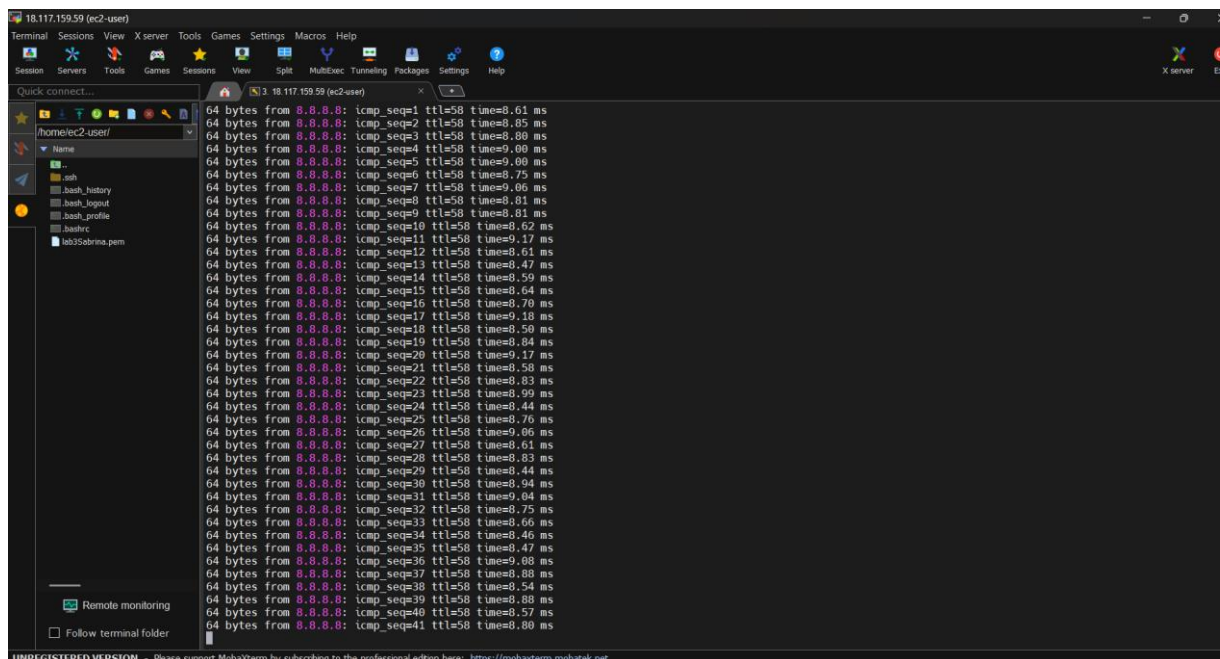
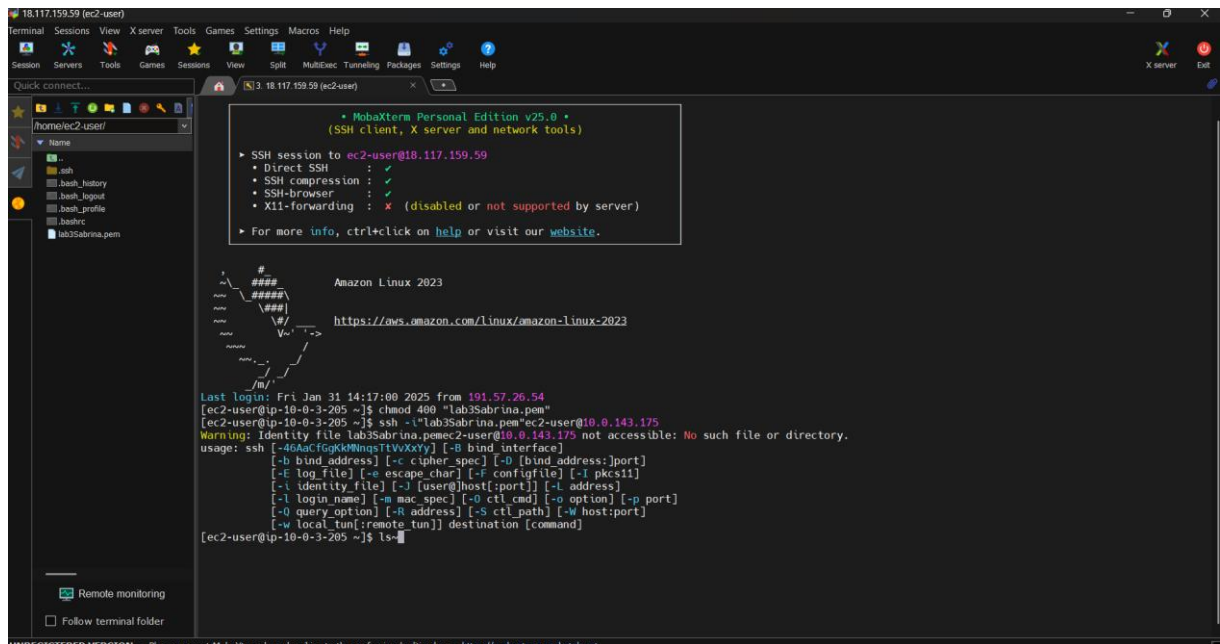
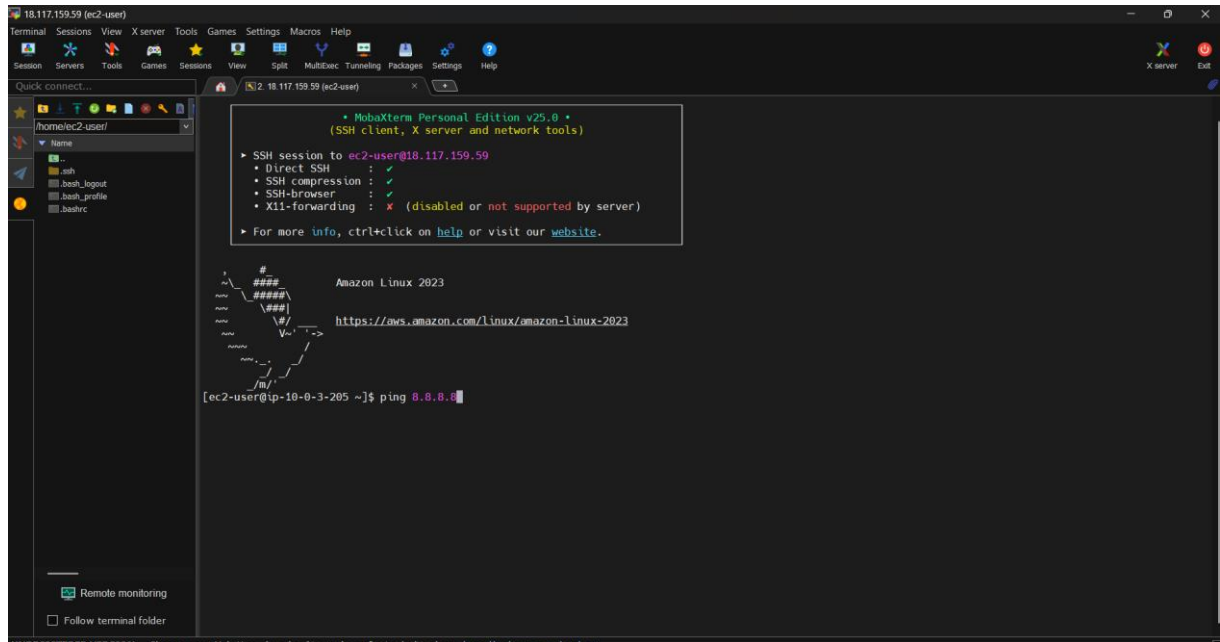
Demonstração do instrutor(a): Configurar um Nat Gateway para acesso da instância de Banco de Dados a internet.

Observações:

- Lembre-se de **encerrar as instâncias EC2** quando não estiverem em uso para evitar custos.
- Após concluir as tarefas, você pode **excluir os recursos criados** neste laboratório, como as instâncias EC2, o Internet Gateway (criado automaticamente com a VPC), as sub-redes e a própria VPC.
- **Atenção:** Exclua os recursos na ordem inversa da criação para evitar erros. Exclua primeiro as instâncias, depois o EIP (se criado), depois os grupos de segurança, e por fim a VPC (que excluirá automaticamente as sub-redes e o Internet Gateway).



Architected Solutions AWS



Documentação Adicional:

- **VPC:** <https://docs.aws.amazon.com/vpc/>
- **EC2:** <https://docs.aws.amazon.com/ec2/>

- **Grupos de Segurança:**
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html
- **MobaXterm:** <https://mobaxterm.mobatek.net/>

Após concluir as tarefas, você pode excluir os recursos criados neste laboratório, como as instâncias EC2, o NAT Gateway, o Internet Gateway, as sub-redes e a VPC.