

Proteção de dados na nuvem

1) Crie 1 bucket no serviço S3

Amazon S3

Buckets

Pontos de acesso

Pontos de acesso Lambda de objeto

Pontos de acesso de várias regiões

Operações em lotes

Analizador de acesso para S3

Configurações de bloqueio do acesso público desta conta

Storage Lens

Painéis

Configurações do AWS Organizations

Recurso em destaque

AWS Marketplace para S3

Visualizar painel do Storage Lens

Armazenamento total

Quantidade de objetos

Tamanho médio do objeto

Você pode habilitar métricas avançadas na configuração "default-account-dashboard".

11,2 MB

9,3 k

1,2 KB

Buckets (3)

Info

Os buckets são contêineres para dados armazenados no S3. Saiba mais

Recarregar

Copiar ARN

Vazio

Excluir

Criar bucket

Encontrar buckets por nome

	Nome	Região da AWS	Acesso	Data de criação
<input type="radio"/>	aws-cloudtrail-logs-104512342307-cda9e845	Leste dos EUA (Norte da Virgínia) us-east-1	Bucket e objetos não públicos	23 Jun 2022 08:00:52 PM -03
<input type="radio"/>	aws-cloudtrail-logs-104512342307-f561a887	Leste dos EUA (Norte da Virgínia) us-east-1	Bucket e objetos não públicos	23 Jun 2022 07:11:32 PM -03
<input type="radio"/>	aws-cloudtrail-logs-104512342307-resolucao	Leste dos EUA (Norte da Virgínia) us-east-1	Bucket e objetos não públicos	23 Jun 2022 08:45:37 PM -03

Amazon S3

Buckets

Criar bucket

Criar bucket

Info

Os buckets são contêineres para dados armazenados no S3. Saiba mais

Configuração geral

Nome do bucket

aula-teste

O nome do bucket deve ser exclusivo e não deve conter espaços ou letras maiúsculas. Consulte as regras de nomenclatura de bucket

Região da AWS

Leste dos EUA (Norte da Virgínia) us-east-1

Copiar configurações do bucket existente - opcional

Somente as configurações de bucket na configuração a seguir são copiadas.

Escolher bucket

Propriedade de objeto

Info

Controlar a propriedade de objetos gravados nesse bucket a partir de nossas contas da AWS e o uso de listas de controle de acesso (ACLs). A propriedade do objeto determina quem pode acessar e a quem são os objetos.

☒ ACLs desabilitadas (recomendado)

Todos os objetos nesse bucket são de propriedade dessa conta. O acesso a esse bucket e aos objetos é gerenciado usando apenas políticas.

☐ ACLs habilitadas

Os objetos nesse bucket podem ser de propriedade de outras contas da AWS. O acesso a esse bucket e aos objetos pode ser gerenciado usando ACLs.

Propriedade do objeto

Imposto pelo proprietário do bucket

Configurações de bloqueio do acesso público deste 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 que o acesso público a esse bucket e todos os seus objetos seja bloqueado, ative a opção de Bloquear todo o acesso público. Essas configurações serão aplicadas apenas a esse bucket e aos 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 funcionando corretamente sem acesso público. Caso precise de algum nível de acesso público a esse bucket ou aos objetos que ele contém, é possível personalizar as configurações individuais abaixo para que atendam aos 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 não é independente 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 listas ou objetos recém-adicionadas e impedirá a criação de novas ACLs de acesso público para listas 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 (ACL)

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 concedam acesso público a buckets e objetos.

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 todos os versões de cada objeto armazenado no bucket do Amazon S3. Com o versionamento, você pode recuperar facilmente objetos não intencionais de upload e falhas de aplicação. Saiba mais

Versionamento de bucket

☒ Desativar

☐ Ativar

Tags (0) - opcional

Adicionar o custo de armazenamento ou outros critérios marcando seu bucket. Saiba mais

Limiting file uploads selected? Find it in the new Unified Settings

Amazon S3 > Buckets > aula-teste4

aula-teste4

Info

Objetos

Propriedades

Permissões

Métricas

Gerenciamento

Pontos de acesso

Visão geral das permissões

Acesso

Bucket e objetos não públicos

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

Editar

Bloquear todo o acesso público

Ativar

Configurações de bloqueio do acesso público individuais deste bucket

Política do bucket

Editar

Excluir

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

Para determinar quais configurações estão ativas, verifique as configurações de bloqueio do acesso público deste bucket. Saiba mais sobre como usar o Bloqueio de acesso público do Amazon S3

Nenhuma política a ser exibida.

Copiar

Amazon S3 > Buckets > aula-teste4 > Editar propriedade do objeto

Editar propriedade do objeto

Info

Propriedade do objeto

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

ACLs desabilitadas (recomendado)

Todos os objetos nesse bucket são de propriedade dessa conta. O acesso a esse bucket e seus objetos é especificado usando apenas políticas.

ACLs habilitadas

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

Habilitar ACLs desativa a configuração imposta pelo proprietário do bucket em relação à propriedade do objeto

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

Reconheço que as ACLs serão restauradas.

Propriedade de objeto

Proprietário do bucket preferido

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

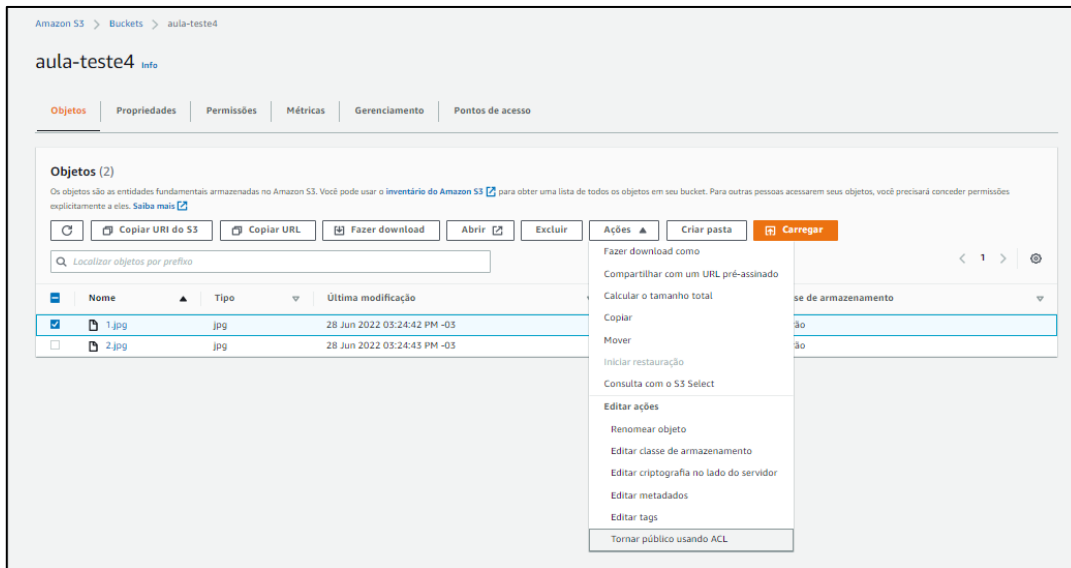
Autor do objeto

O autor do objeto continua sendo o proprietário do objeto.

Para impor a propriedade do objeto somente para novos objetos, é necessário que a política do bucket especifique que a ACL pré-configurada "bucket-owner-full-control" é necessária para carregar objetos. Saiba mais

Cancelar

Salvar alterações

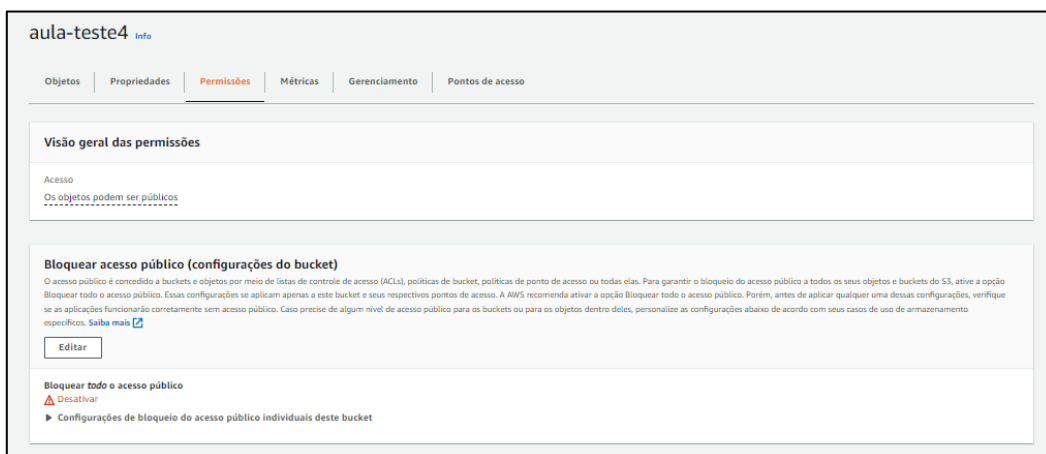


O segundo objeto continua privado? O que aconteceu?

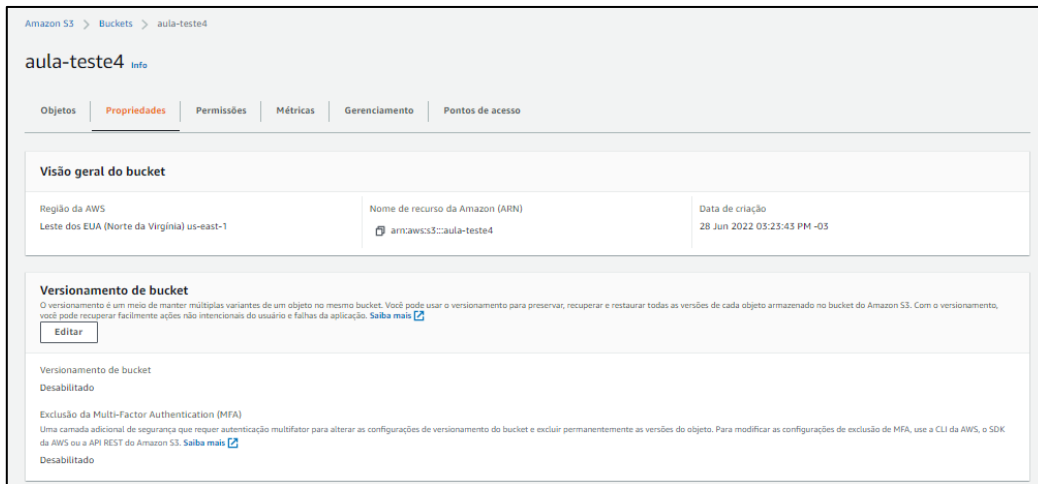
2) Associe uma política de bucket que só permite acesso ao seu próprio IP. Consulte esta documentação: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html#example-bucket-policies-use-case-3>

2.1) Teste o acesso do seu IP e de um outro IP (pode ser do seu celular 4G, por exemplo). O que aconteceu?

2.1.1) Feche todo o acesso público do bucket



2.1) Ative o versionamento e apague um arquivo

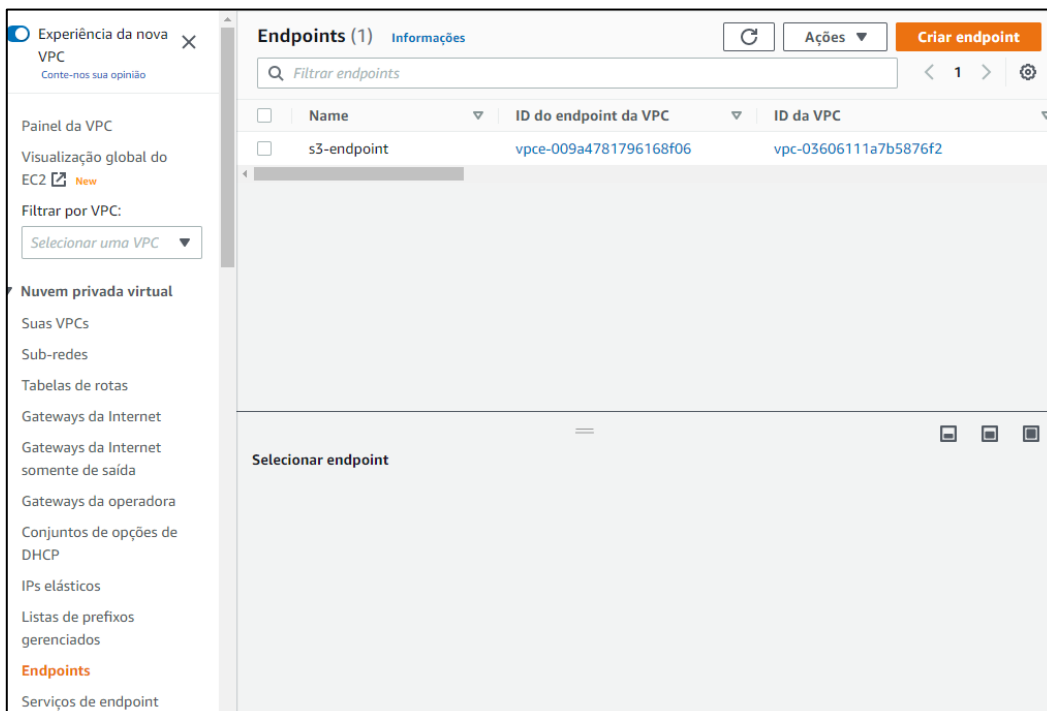


2.2) Tente restaurar o arquivo excluído. O que aconteceu?

3) Suba uma instância EC2 pequena usando configurações padrão. Acesse o terminal desta instância e tente executar o seguinte comando de cópia: `aws s3 cp s3://nome-do-bucket/objeto.jpg /tmp/objeto.jpg` O que aconteceu?

3.2) Na mesma linha de comando, tente executar o seguinte comando: `traceroute nomedobucket.s3.amazonaws.com` Qual rota foi usada para buscar o arquivo?

3.2.1) Crie um vpc endpoint para o S3



VPC > Endpoints > Criar endpoint

Criar endpoint Informações

Existem três tipos de endpoints da VPC: endpoints de interface, endpoints do balancador de carga de gateway e endpoints de gateway. Os endpoints de interface e endpoints de balancador de carga de gateway são desenvolvidos pelo AWS PrivateLink e usam uma interface de rede elástica (ENI) como ponto de entrada para o tráfego destinado ao serviço. Os endpoints de interface normalmente são acessados usando o nome DNS público ou privado associado ao serviço, enquanto os endpoints de gateway e endpoints de balancador de carga de gateway funcionam como destino para uma rota na tabela de rotas para o tráfego destinado ao serviço.

Configurações de endpoint

Etiqueta de nome - opcional
Crie uma etiqueta com uma chave de "Nome" e um valor que você especifica.

novovpc-endpoint

Categoria de serviço
Selecione a categoria do serviço

☒ Serviços da AWS
Serviços fornecidos pela Amazon

☐ Serviços de parceiros do PrivateLink Ready
Serviços com uma designação AWS Service Ready

☐ Serviços da AWS Marketplace
Serviços adquiridos por meio do AWS Marketplace

☐ Outros serviços de endpoint
Encontre serviços compartilhados com você por nome de serviço

Serviços (1/3)

Filtrar serviços

Nome do serviço: com.amazonaws-us-east-1:cs [X] Limpar filtros

Nome do serviço	Proprietário	Tipo
<input checked="" type="radio"/> com.amazonaws-us-east-1:cs	amazon	Gateway
<input type="radio"/> com.amazonaws-us-east-1:cs	amazon	Interface
<input type="radio"/> com.amazonaws-us-east-1:cs-outposts	amazon	Interface

VPC

Selecione a VPC na qual criar o endpoint

VPC
A VPC em que seu endpoint será criado.

vpc-0506111a7b5876f2

Tabelas de rotas (1/1) Informações

Filtrar tabelas de rotas

Nome	ID da tabela de rotas	Principal
<input checked="" type="checkbox"/> -	rtb-028b199fa118ba40	Sim

Quando você usa um endpoint, os endereços IP de origem das instâncias contidas nas sub-redes afetadas para acesso ao serviço da AWS na mesma região são endereços IP privados, e não endereços IP públicos. As conexões existentes de suas sub-redes afetadas para o serviço da AWS que usam endereços IP públicos podem ser descartadas. Verifique se não há tarefas críticas em execução ao criar ou modificar um endpoint.

3.3) Após a criação do endpoint, execute o mesmo traceroute novamente. O que aconteceu?

4) Crie uma chave simétrica no KMS

Key Management Service (KMS)

Chaves gerenciadas pela AWS

Chaves gerenciadas pelo cliente

Armazenamentos de chaves personalizado

KMS > Chaves gerenciadas pelo cliente

Chaves gerenciadas pelo cliente (3) Ações da chave Criar chave

Filtrar chaves por propriedades ou tags

	Aliases	ID da chave	Status	Especificação de chave	Uso da chave
<input type="checkbox"/>	nova	454ff6b1-02ac-4797-807f-afc3e0b69c40	Habilitada	SYMMETRIC_DEFAULT	Criptografar e descriptografar
<input type="checkbox"/>	cloudtrail-key-trilha-bi	52a1500e-5cb6-41f8-a129-8243d3bffa01	Habilitada	SYMMETRIC_DEFAULT	Criptografar e descriptografar
<input type="checkbox"/>	etete	8ea6a9ff-a9cb-42f5-aac1-70fc70a52a9e	Habilitada	SYMMETRIC_DEFAULT	Criptografar e descriptografar

KMS > Chaves gerenciadas pelo cliente > Criar chave

Definir permissões administrativas da chave

Administradores de chaves

Escolha os usuários e as funções do IAM que podem administrar esta chave com a API do KMS. Talvez sejam necessárias permissões adicionais para que os usuários ou funções possam administrar essa chave a partir deste console. [Saiba mais](#)

Q

< 1 2 >

Nome

Caminho

Tipo

☐

EMR_DefaultRole

/

Role

☐

EMR_EC2_DefaultRole

/

Role

☐

LabRole

/

Role

☐

robomaker_students

/

Role

☐

vocareum

/

Role

☒

voclabs

/

Role

☐

vocstartsoft

/

Role

Exclusão de chaves

☒ Permitir que administradores de chaves excluam esta chave.

Cancelar

Anterior

Próximo

KMS > Chaves gerenciadas pelo cliente > Criar chave

Etapa 1

Configurar chave

Etapa 2

Adicionar rótulos

Etapa 3

Definir permissões administrativas da chave

Etapa 4

Definir permissões de uso da chave

Etapa 5

Revisar

Definir permissões de uso da chave

Esta conta

Selecione os usuários e as funções do IAM que podem usar a chave do KMS em operações de criptografia. [Saiba mais](#)

Q

< 1 2 >

Nome

Caminho

Tipo

☐

EMR_DefaultRole

/

Role

☐

EMR_EC2_DefaultRole

/

Role

☐

LabRole

/

Role

☐

robomaker_students

/

Role

☐

vocareum

/

Role

☒

voclabs

/

Role

☐

vocstartsoft

/

Role

Outras contas da AWS

Especifique as contas da AWS que podem usar essa chave. Os administradores das contas que você especificar são responsáveis por gerenciar as permissões para que os usuários e as funções do IAM possam usar essa chave. [Saiba mais](#)

Adicionar outra conta da AWS

Cancelar

Anterior

Próximo

KMS > Chaves gerenciadas pelo cliente > Criar chave

Configurar chave

Tipo de chave [Ajude-me a escolher](#)

☒ **Simétrica**
 Uma única chave usada para criptografar e descriptografar dados ou gerar e verificar códigos HMAC

☐ **Assimétrica**
 Um par de chaves públicas e privadas usado para criptografar e descriptografar dados ou assinar e verificar mensagens

Uso da chave [Ajude-me a escolher](#)

☒ **Criptografar e descriptografar**
 Use a chave somente para criptografar e descriptografar dados.

☐ **Gerar e verificar MAC**
 Use a chave apenas para gerar e verificar códigos de autenticação de mensagem por hash (HMAC).

► **Opções avançadas**

Cancelar **Próximo**

5) habilite a criptografia usando uma chave kms no S3.

Amazon S3 > Buckets > aula-teste4 > Editar criptografia padrão

Editar criptografia padrão

Criptografia padrão
 Criptografar automaticamente novos objetos armazenados neste bucket. [Saiba mais](#)

Criptografia no lado do servidor

☐ Desativar
☒ **Ativar**

Tipo da chave de criptografia
 Para fazer upload de um objeto com uma chave de criptografia fornecida pelo cliente (SSE-C), use a CLI da AWS, o SDK da AWS ou a API REST do Amazon S3.

☐ Chaves gerenciadas pelo Simple Storage Service (Amazon S3) (SSE-S3)
 Uma chave de criptografia que o Amazon S3 cria, gerencia e usa para você. [Saiba mais](#)

☒ **Chave do AWS Key Management Service (SSE-KMS)**
 Uma chave de criptografia protegida pelo AWS Key Management Service (AWS KMS). [Saiba mais](#)

Chave do AWS KMS

☐ Chave gerenciada pela AWS (aws/s3)
 amzaws:kms:us-east-1:104512342307:alias/aws/s3

☒ **Escolher entre suas chaves do AWS KMS**

☐ Inserir ARN da chave do AWS KMS

Chave do AWS KMS

amzaws:kms:us-east-1:104512342307:key/8b226...

Chave do bucket
 Reduza os custos de criptografia diminuindo as chamadas para o AWS KMS para novos objetos neste bucket. Para especificar uma configuração de chave de bucket para um objeto, use a CLI da AWS, o SDK da AWS ou a API Rest do Amazon S3. [Saiba mais](#)

☐ Desativar
☒ **Ativar**

Cancelar **Salvar alterações**

5.1) Habilite a criptografia na instância EC2 criada anteriormente no exercício 3. Use a seguinte documentação:

https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/EBSEncryption.html#encrypt-on-parameters

Quais passos foram necessários para criptografar o volume?

5.2) Habilite criptografia em uma instância nova. O que acontece com os snapshots deste tipo de instância?

☐ 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.

▼ Armazenamento (volumes) [Informações](#)

Simplex

Volumes do EBS [Ocultar detalhes](#)

▼ Volume 1 (Raiz da AMI) (Personalizada)

Tipo de armazenamento Informações EBS	Nome do dispositivo - required Informações /dev/xvda	Snapshot Informações snap-08f1069dfde2007ba
Tamanho (GiB) Informações 8	Tipo de volume Informações gp2	IOPS Informações 100 / 3000
Excluir no encerramento Informações Yes	Criptografado Informações Yes	Chave do KMS Informações chave-aula ID da chave: Sb2264fa-f0a9-4f...

ⓘ Os clientes qualificados para o nível gratuito podem obter até 30 GB de armazenamento de uso geral (SSD) ou armazenamento magnético do EBS

[Adicionar novo volume](#)

Sistemas de arquivos [Mostrar detalhes](#)

▼ Resumo

Número de instâncias [Informações](#)

1

Imagem do software (AMI)
 Amazon Linux 2 Kernel 5.10 AMI... [Ver mais](#)
 ami-0c9f7528f583bf9a

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

Firewall (grupo de segurança)
 Novo grupo de segurança

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

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

[Cancelar](#)
[Executar instância](#)

6) Crie um banco de dados relacional PostgreSQL.

RDS > Create database

Criar banco de dados

Escolher um método de criação de banco de dados [Informações](#)

☒ **Criação padrão**
 Defina todas as opções de configuração, incluindo as de disponibilidade, segurança, backups e manutenção.

☐ **Criação fácil**
 Use as configurações recomendadas de melhores práticas. Algumas opções de configuração podem ser alteradas após a criação do banco de dados.

Opções do mecanismo

Tipo de mecanismo [Informações](#)

☐ Amazon Aurora

☐ MySQL

☐ MariaDB

☒ PostgreSQL

☐ Oracle

☐ Microsoft SQL Server

Versão

PostgreSQL 13.4-R1

Modelos

Escolha um modelo de exemplo para atender a seu caso de uso.

☐ **Produção**
 Use padrões para alta disponibilidade e desempenho rápido e consistente.

☐ **Desenvolvimento/Teste**
 Esta instância é planejada para uso de desenvolvimento fora de um ambiente de produção.

☒ **Nível gratuito**
 Use o nível gratuito do RDS para desenvolver novos aplicativos, testá-los ou obter uma experiência prática com o Amazon RDS. [Informações](#)

Configurações

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

Digite um nome para a instância de banco de dados. O nome deve ser exclusivo entre todas as instâncias de banco de dados de propriedade de sua conta da AWS na região atual da AWS.

database-1

O identificador da instância de banco de dados não diferencia maiúsculas de minúsculas, mas é armazenado com todas as letras minúsculas (como em "mydbinstance"). Restrições: 1 a 60 caracteres alfanuméricos ou hífen. O primeiro caractere deve ser uma letra. Não pode conter dois hífens consecutivos. Não pode terminar com um hífen.

▼ Configurações de credenciais

Nome do usuário principal [Informações](#)

Digite um ID de login para o usuário principal de sua instância de banco de dados.

postgres

De um a 16 caracteres alfanuméricos. O primeiro caractere deve ser uma letra.

☐ Gerar uma senha automaticamente

O Amazon RDS pode gerar uma senha para você, ou você pode especificar sua própria senha.

Senha principal [Informações](#)

Restrições: pelo menos oito caracteres ASCII imprimíveis. Não pode conter nenhum dos seguintes: / (barra), ' (aspas simples), " (aspas duplas) ou @ (arroba).

Confirmar senha [Informações](#)

Configuração da instância

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

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)

Armazenamento

Tipo de armazenamento [Informações](#)

SSD de uso geral (gp2)

Performance de linha de base determinada pelo tamanho do volume

Armazenamento alocado

20 GiB

Limite: 20 GiB. Máximo: 16,384 GiB

Armazenamento alocado mais alto pode melhorar a performance de IOPS.

Escalabilidade automática do armazenamento [Informações](#)

Permite manter a escalabilidade dinâmica de seu armazenamento de banco de dados de acordo com as necessidades do seu aplicativo.

☒ Habilitar escalabilidade automática do armazenamento

Habilita mais recursos para que o armazenamento aumente depois que o limite especificado for excedido.

Limite máximo de armazenamento [Informações](#)

As seguintes regras aplicáveis quando seu banco de dados escalar automaticamente para o limite especificado

1000 GiB

Limite: 22 GiB, máximo: 16,384 GiB

Conectividade

Virtual private cloud (VPC) [Informações](#)

A VPC que define o ambiente de rede virtual para sua instância de banco de dados.

Default VPC (vpc-0360611a7b5876f2)

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

☒ Depois de criar o banco de dados, não é possível alterar a VPC.

Grupo de sub-redes [Informações](#)

O grupo de sub-redes de banco de dados que define as sub-redes e os intervalos de IP que a instância de banco de dados pode usar na VPC selecionada.

default-vpc-0360611a7b5876f2

Acesso público [Informações](#)

☐ Sim

As instâncias e os dispositivos da Amazon EC2 fora da VPC podem se conectar ao banco de dados. Escolha um ou mais grupos de segurança da VPC que especifiquem quais instâncias e dispositivos da EC2 dentro da VPC podem se conectar ao banco de dados.

☒ Não

O RDS não exibirá um endereço IP público ao banco de dados. Somente as instâncias e dispositivos da Amazon EC2 dentro da VPC podem se conectar ao banco de dados.

Grupo de segurança da VPC

Escolha um grupo de segurança da VPC para permitir o acesso ao seu banco de dados. Certifique-se de que as regras do grupo de segurança permitam o tráfego de entrada necessário.

☒ Seleccionar existente

Seleccionar grupo de segurança de VPC existentes

☐ Criar novo

Criar grupo de segurança da VPC

Grupos de segurança da VPC existentes

Seleccionar grupos de segurança da VPC

default X

Zona de disponibilidade [Informações](#)

Sem preferência

► Configuração adicional

Autenticação de banco de dados

nova instância de banco de dados usando a Autenticação Federada.

▼ **Configuração adicional**
 Opções de banco de dados, criptografia desativada, backup desativado, retroware desativado, Insights de Performance desativado, Monitoramento avançado desativado, manutenção, CloudWatch Logs, exclusão proteção desativado.

Opções de banco de dados

Nome do banco de dados inicial [Informações](#)

Se você não especificar um nome de banco de dados, o Amazon RDS não criará um banco de dados.

Grupo de parâmetros de banco de dados [Informações](#)

Grupo de opções [Informações](#)

Backup

☐ Habilitar backups automatizados.
 Cria um snapshot ponto-em-noze do seu banco de dados.

Criptografia

☐ Habilitar criptografia
 A opção de criptografia a respectiva instância. Os IDs e a chave de chave-mestres são exibidos na lista após terem sido criados usando o console do AWS Key Management Service. [Informações](#)

Insights de Performance [Informações](#)

☐ Ativar o Performance Insights [Informações](#)

Monitoramento

☐ Habilitar monitoramento avançado
 É desativado automaticamente quando você desliga um ou mais processos ou threads ou a CPU.

Exportações de log
 Selecione os tipos de log para publicar no Amazon CloudWatch Logs.

☐ Log do PostgreSQL

☐ Log de upgrade

Função do IAM
 A seguinte função vinculada ao serviço é usada para a publicação de logs no CloudWatch Logs.

ⓘ Certifique-se de que os logs dos tipos geral, consulta lenta e auditoria estejam ativados. Os logs de erros estão habilitados por padrão. Saiba mais

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 e versões que foram lançadas. Os upgrades automáticos ocorrem durante a janela de manutenção do banco de dados.

Janela de manutenção [Informações](#)
 Selecione o período no qual você deseja que as atualizações 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.

6.1)Habilite a criptografia usando chave kms no RDS para o banco de dados criado. Foi possível? Por que? Consulte a seguinte documentação:
https://docs.aws.amazon.com/pt_br/AmazonRDS/latest/UserGuide/Overview.Encryption.html