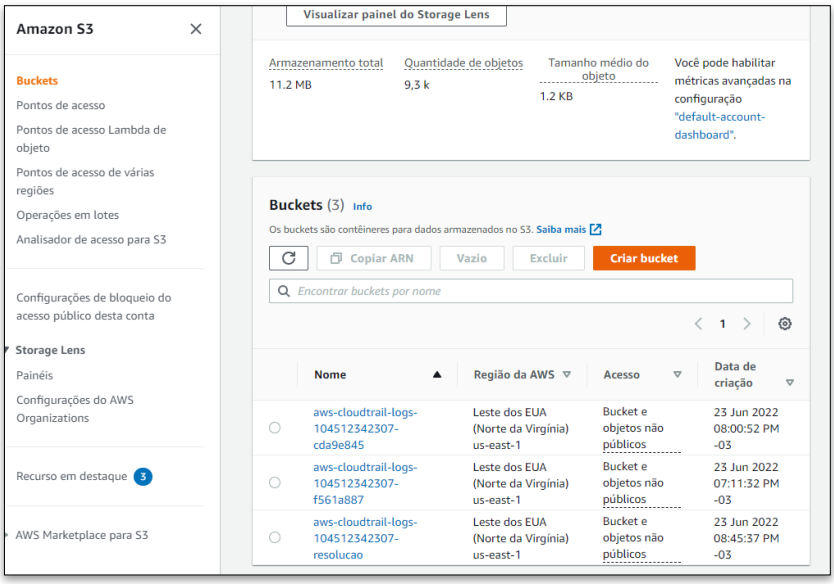
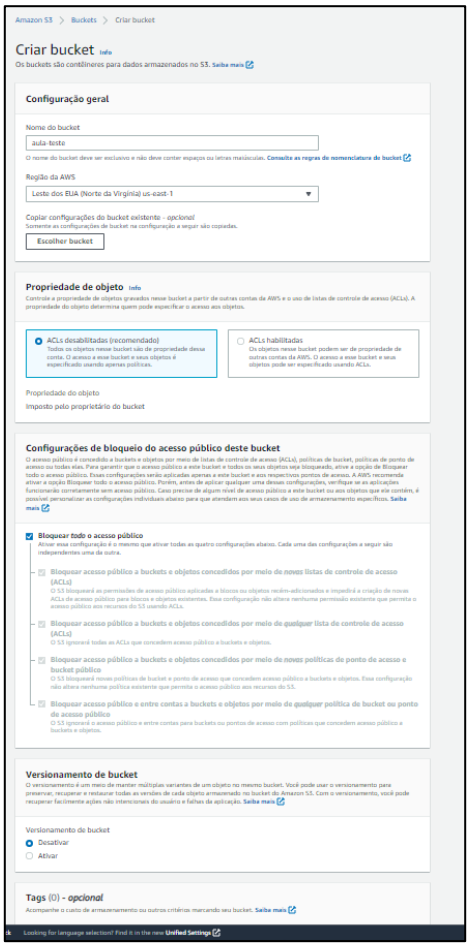
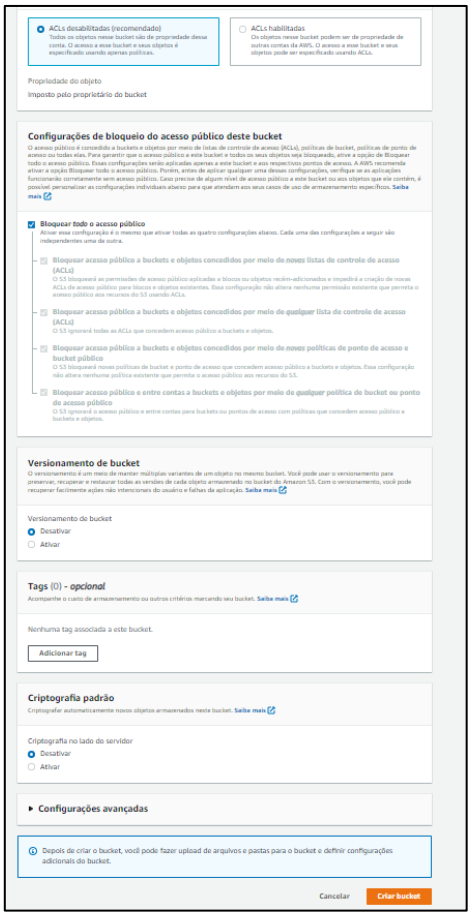
# Proteção de dados na nuvem

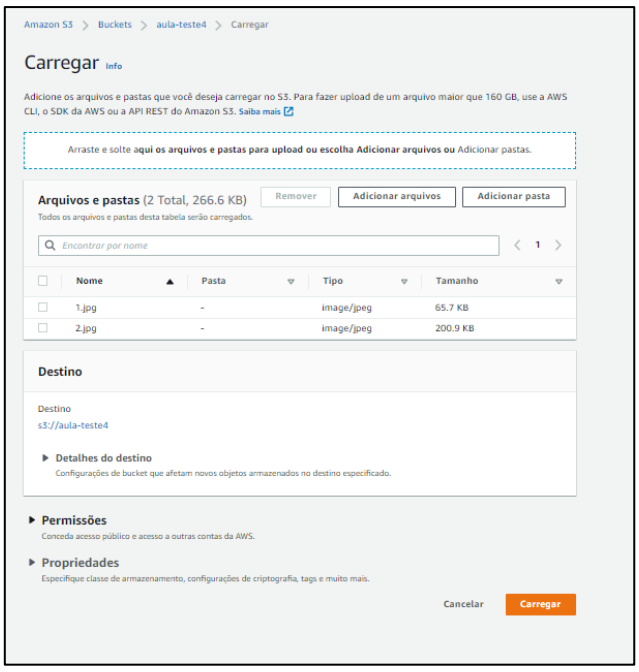
1)Crie 1 bucket no serviço S3

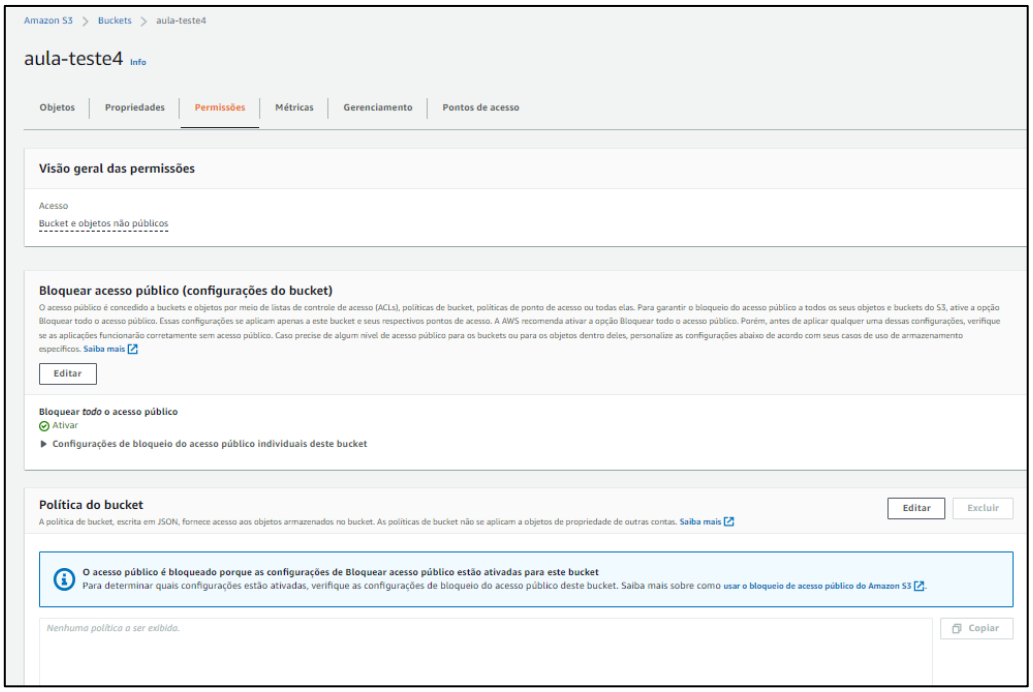


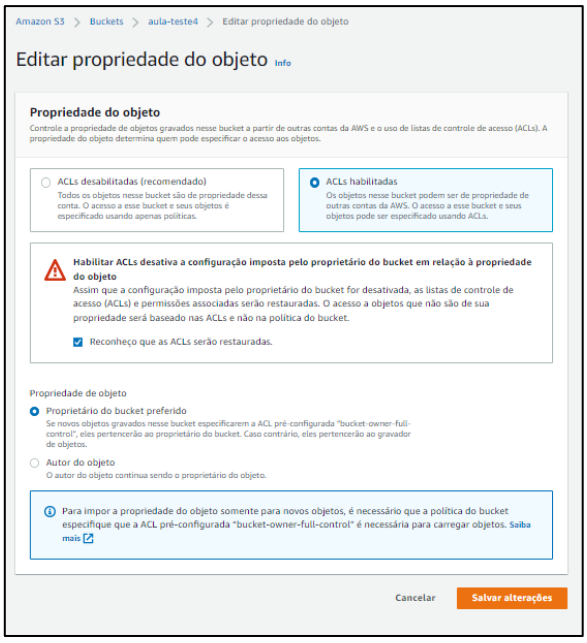



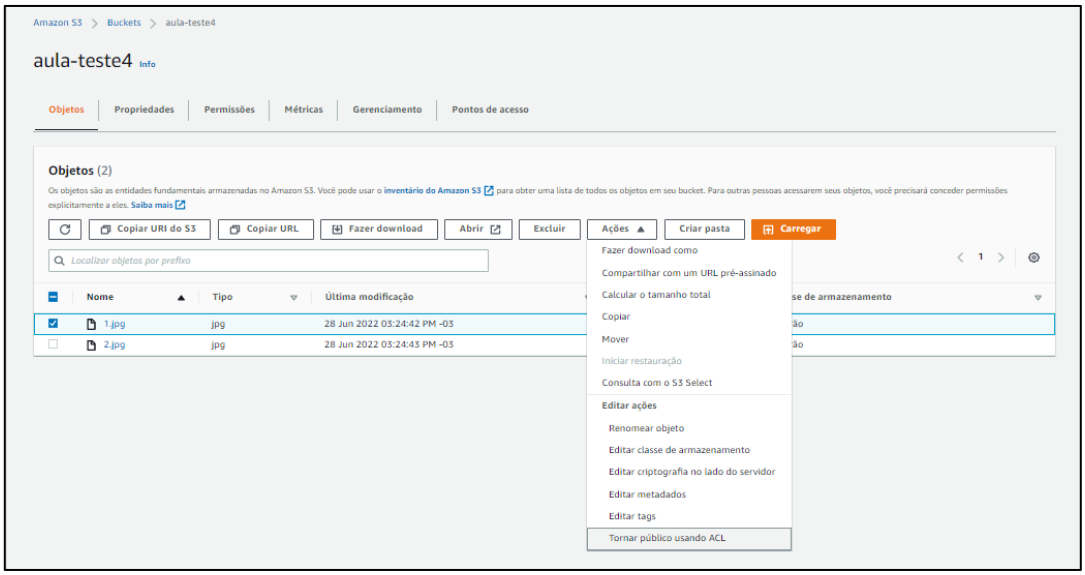



1.1)Faça upload de 2 arquivos de imagens. Torne um deles público.




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
A política de bucket, escrita em JSON, fornece acesso aos objetos armazenados no bucket. As políticas de bucket não se aplicam a objetos de propriedade de outras contas. Saiba mais
Editar
Excluir
O acesso público é bloqueado porque as configurações de Bloquear acesso público estão ativadas para este bucket
Para determinar quais configurações estão ativadas, 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



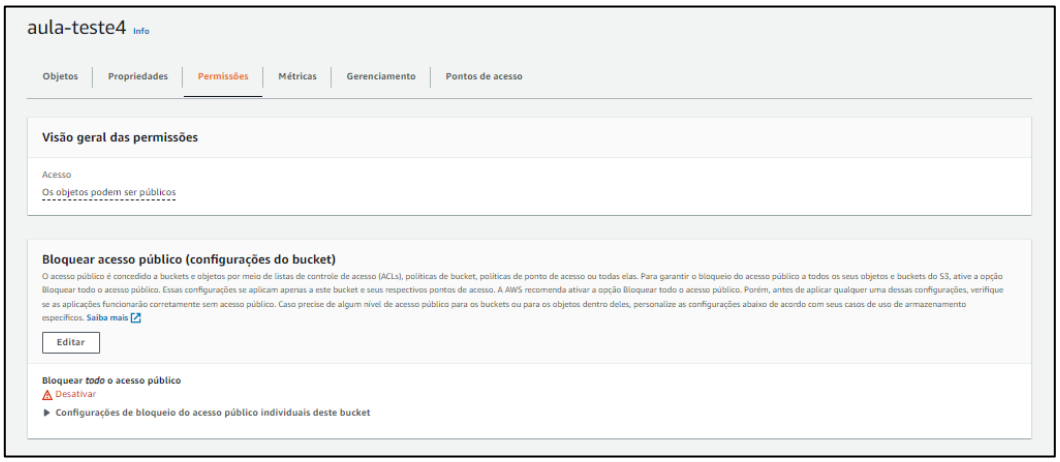

O segundo objeto continua privado? O que aconteceu?

---

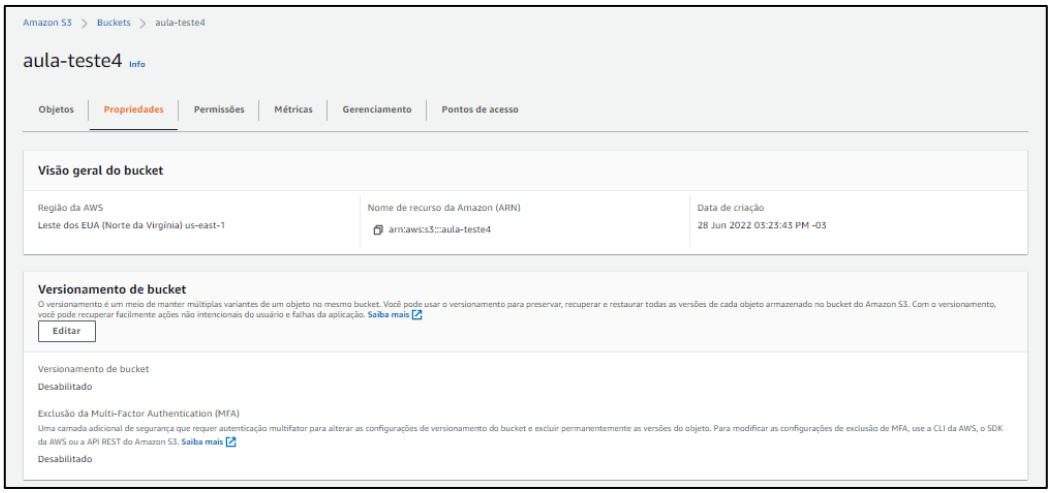
2)Associe uma política de bucket que só permite acesso ao seu próprio IP. Consulte esta documentação: https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html#example-bucket-policies-use-case-3

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



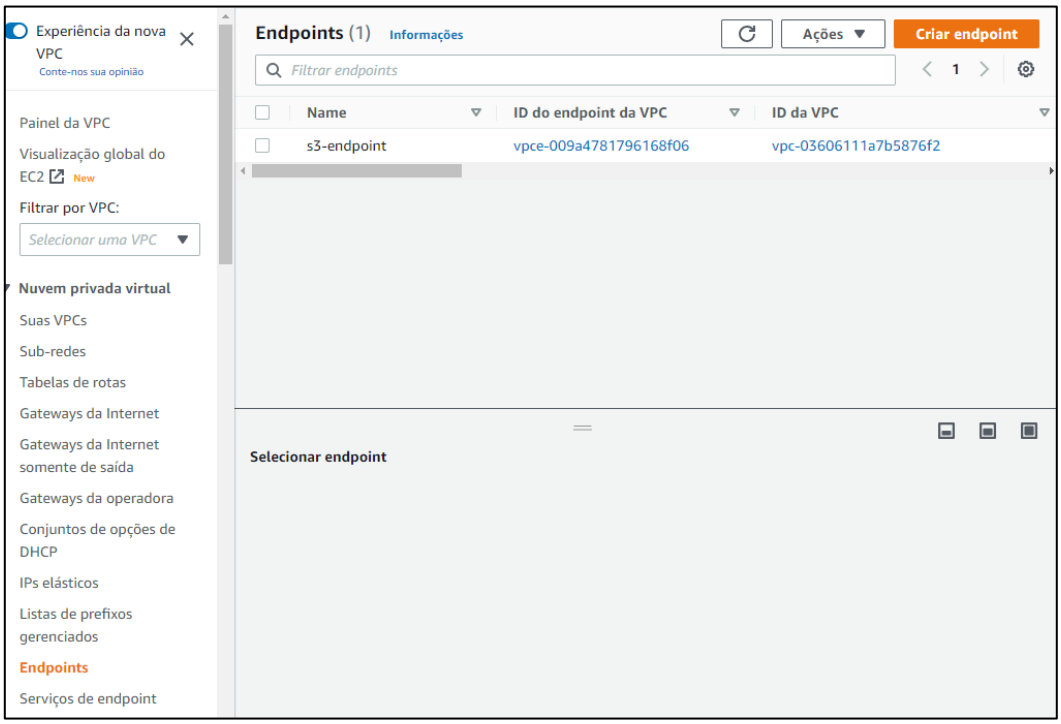

2.2) Tente restaurar o arquivo excluído. O que aconteceu?

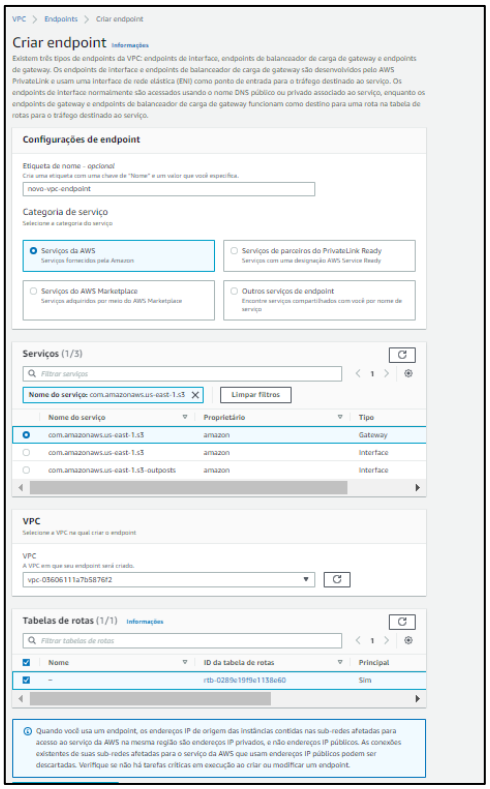
---

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

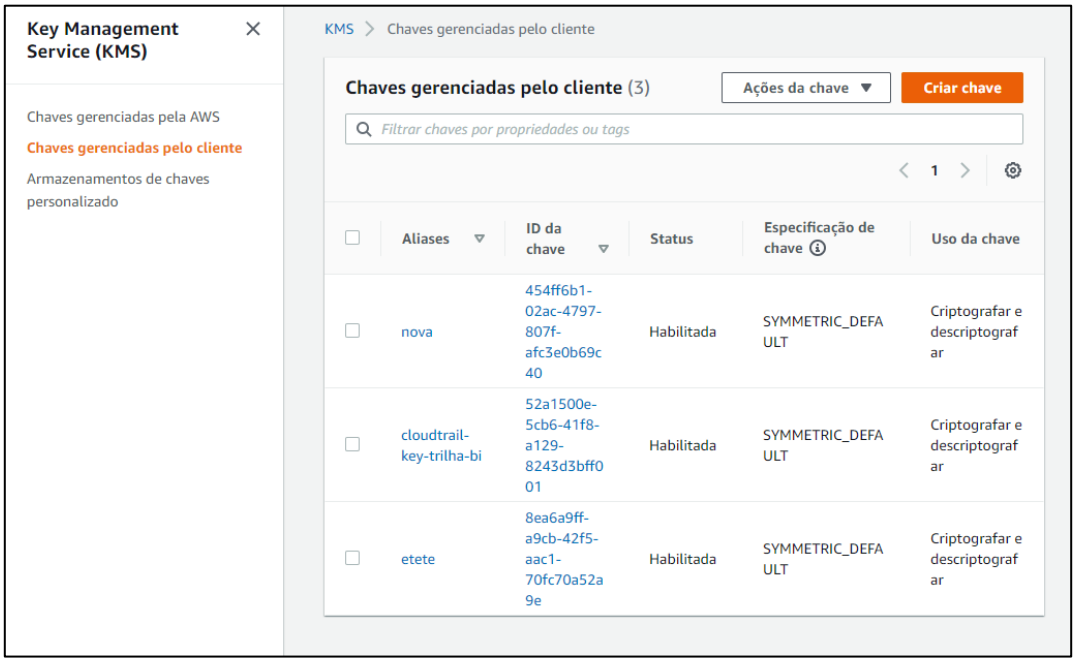


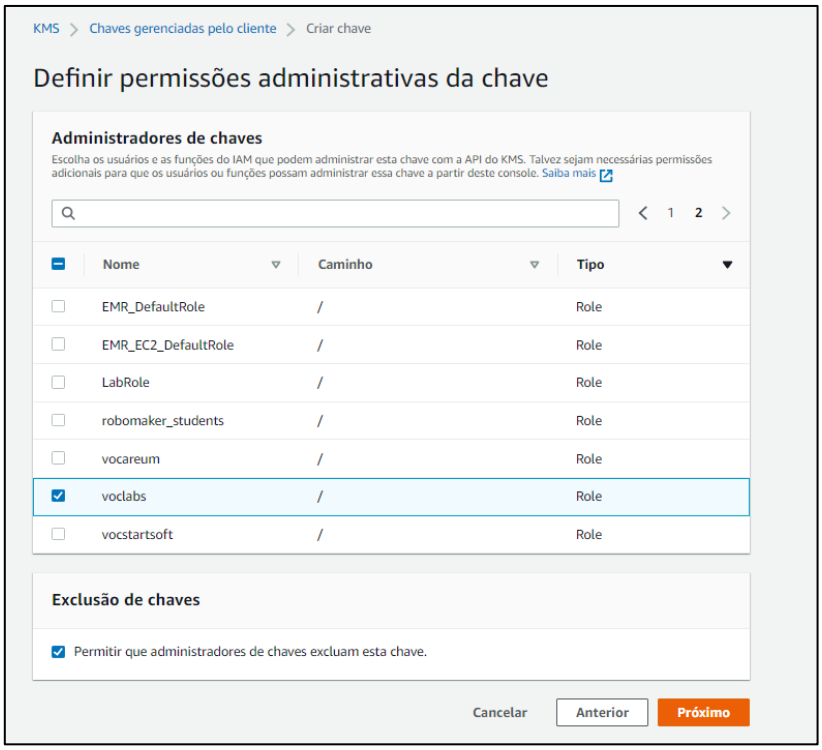


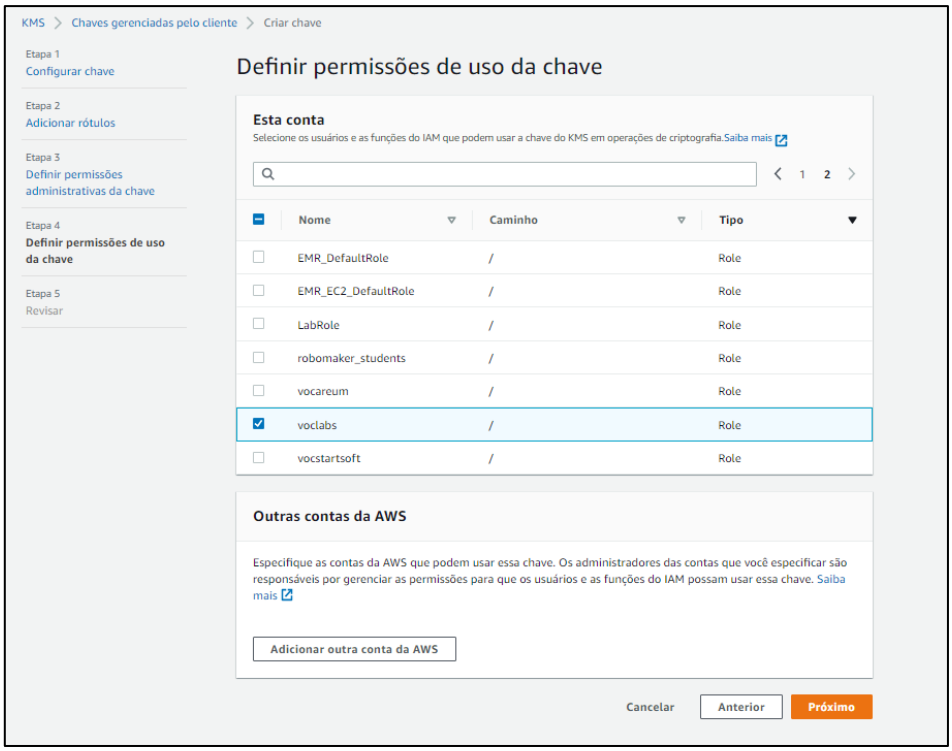

3.3)Após a criação do endpoint, execute o mesmo traceroute novamente. O que aconteceu?

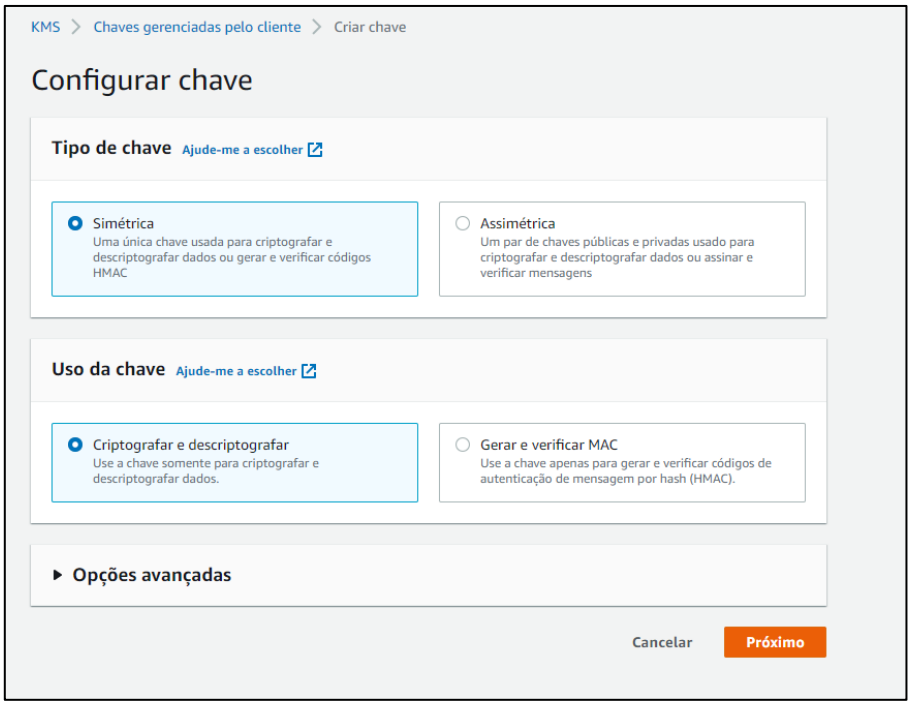
---

4)Crie uma chave simétrica no KMS

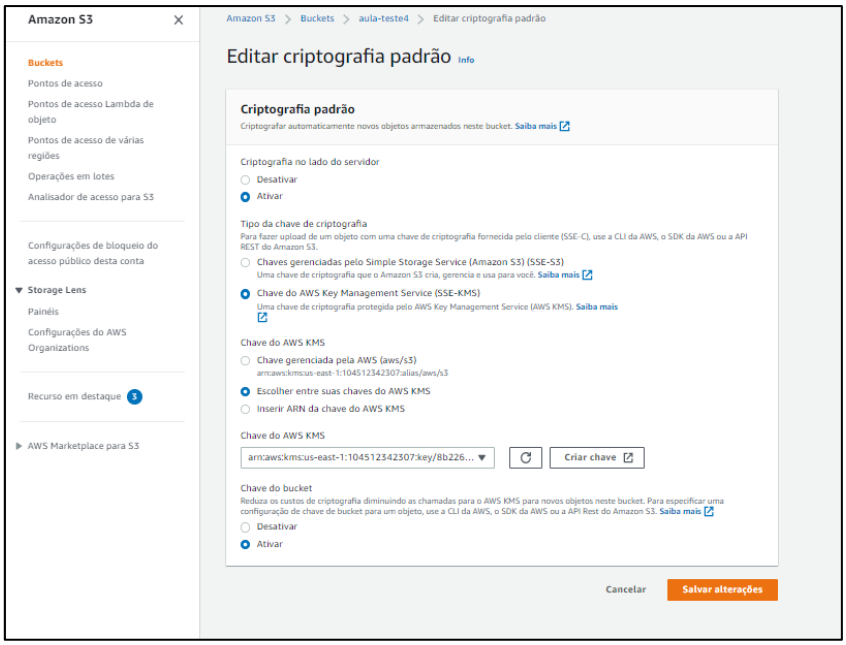



KMS > Chaves gerenciadas pelo cliente > Criar chave
Definir permissões administrativas da chave
Administradores de chaves
Escolha os usuários e as funções do IAM que podem administrar esta chave com a API do KMS. Talvez sejam necessárias permissões adicionais para que os usuários ou funções possam administrar essa chave a partir deste console. Saiba mais
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
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



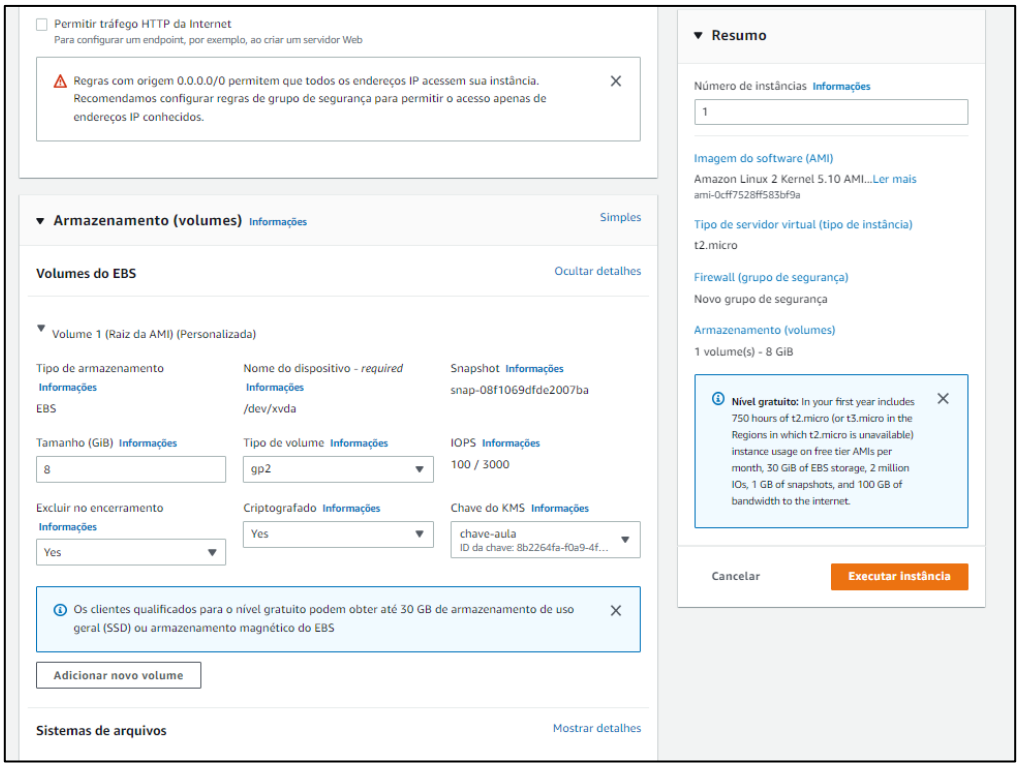

5)habilite a criptografia usando uma chave kms no S3.



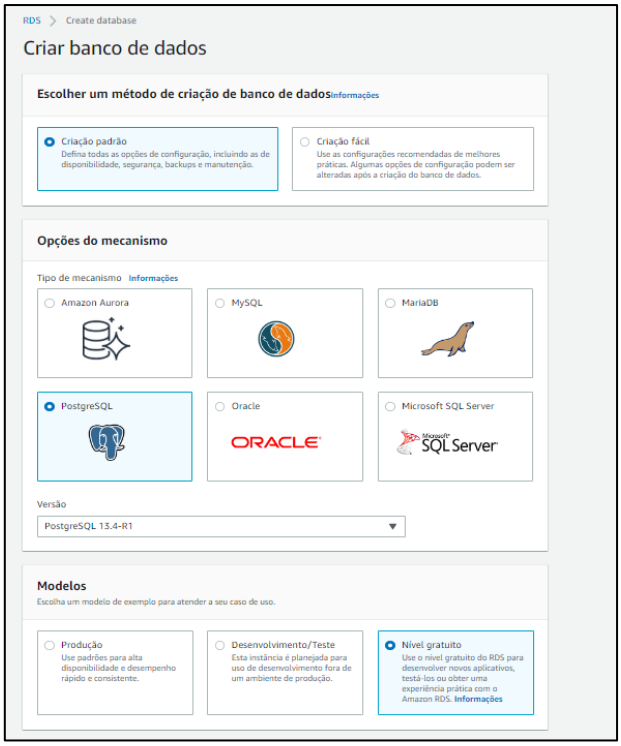

5.1)Habilite a criptografia na instância EC2 criada anteriormente no exercício 3. Use a seguinte documentação:
https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-parameters

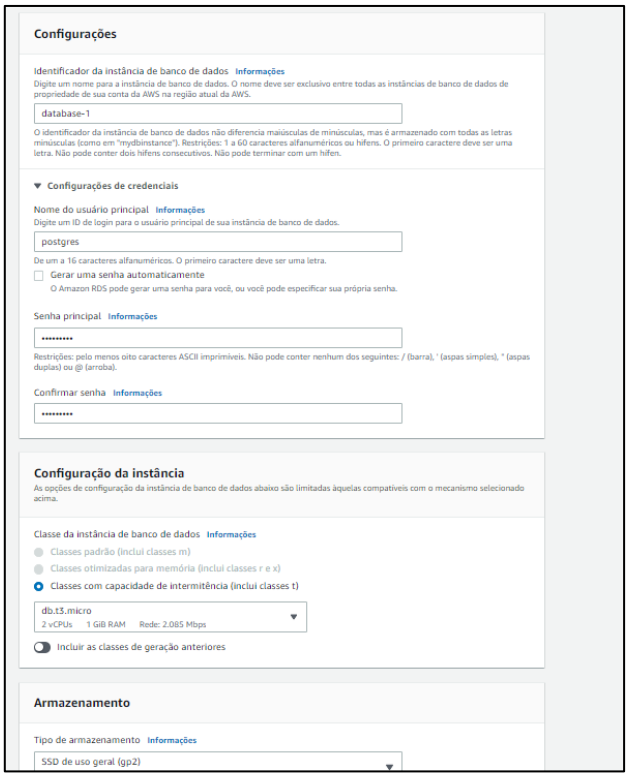
Quais passos foram necessários para criptografar o volume?

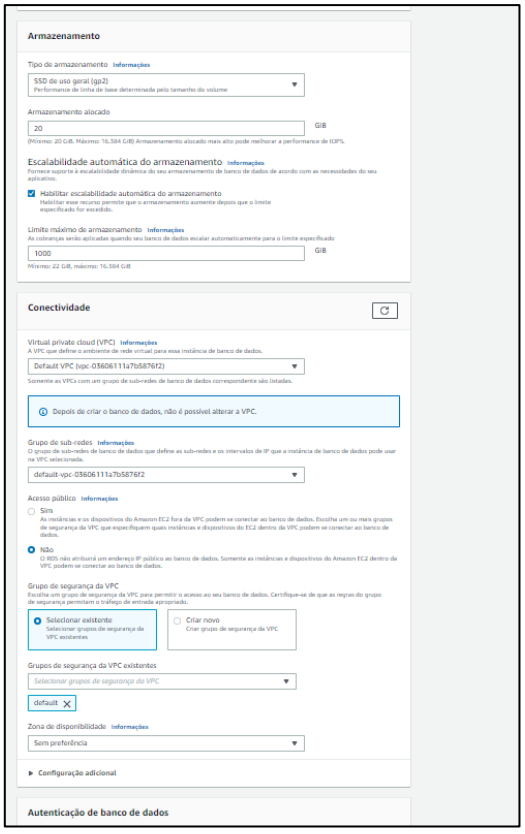
5.2)Habilite criptografia em uma instância nova. O que acontece com os snapshots deste tipo de instância?

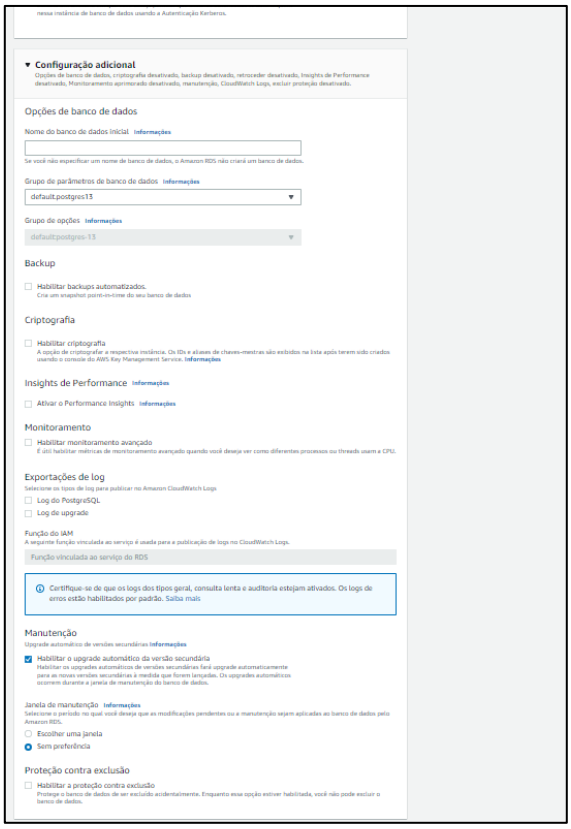



6)Crie um banco de dados relacional PostgreSQL.




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 hífens. 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)
Armazenamento alocado
20
GiB
Escalabilidade automática do armazenamento Informações
Habilitar escalabilidade automática do armazenamento
Limite máximo de armazenamento Informações
1000
GiB
Conectividade
Virtual private cloud (VPC) Informações
Default VPC (vpc-03606111a7b5876f2)
Depois de criar o banco de dados, não é possível alterar a VPC.
Grupo de sub-redes Informações
default-vpc-03606111a7b5876f2
Acesso público Informações
Sim
Não
Grupo de segurança da VPC
Selecionar existente
Criar novo
Grupos de segurança da VPC existentes
Selecionar grupos de segurança da VPC
default
Zona de disponibilidade Informações
Sem preferência
Configuração adicional
Autenticação de 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