Cloud Security - Laboratório 3

1)Crie 1 bucket no serviço S3
1.1)Faça upload de 2 arquivos de imagens. Torne um deles público.
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

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.
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