Describe how to ensure IAM roles and policies (unique by service) are set up.

Reflect on how IAM roles and policies were used in this course.

According to our CORS video this week, If you’re hosting some website on domain1, and domain1 is trying to access a resource on domain2, it is blocked by default by all browsers. CORS on AWS API Gateway should be implemented with appropriate Response Headers for each exposed REST resource. This can be set in permissions, CORS configuration tab for each particular resource. API Gateway enables routes to be configured from URL paths to code, and implement as REST Api.

**What is IAM?**

According to AWS Amazon website, “AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources” (Whitehouse-Grant-Christ).

IAM Helps to implement principle of least privelege in the cloud, while providing fine-grained, secure-by-default authentication and authorization controls.

**What are IAM Policies? Reflect on how IAM roles and policies were used in this course.**

IAM uses users, groups, and permissions can applied to various API calls and lambdas to control authentication (log in) and authorization (who can access what). You can control which users can access specific services, actions they can perform and which particular resources are available via IAM roles and policies. We utilized such policies last week when we created Lambdas and set permissions by attaching IAM policies through the API Gateway, and additionally specified which types of actions these lambdas could perform on our database. Such permissions can also be fine-tuned to control who can launch an Amazon EC2 instance. We set policies to control public access to our S3 bucket, which were not accessible at first. With AWS Cloudtrail you can log IAM and API activity. AWS is secure-by-default with fine-grained access and data locality controls, and provides infrastructure components to build securely by default (Intro to AWS). IAM rotates access keys on VMs, and ensures only trusted users have appropriate access while the developer focuses on the features.

Introduction to AWS iam - identity and access ... - youtube. (n.d.). Retrieved April 8, 2022, from <https://www.youtube.com/watch?v=Ul6FW4UANGc>

AWS. (n.d.). Policies and permissions in IAM. Retrieved from AWS Documentation: <https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html>

Whitehouse-Grant-Christ, I. H. V. (2011). IAM. Amazon. Retrieved April 7, 2022, from <https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>