Week 3 Readings/Resources

Amazon DynamoDB

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity make it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.Pricing for DynamoDB includes a non-expiring free tier allotment. **AWS Identity and Access Management**

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. We typically use credentials from *IAM Users*or *IAM Roles* to authenticate with AWS when making API calls. We control the permissions for which API actions those Users or Roles can perform with *IAM Policies*.

In this course we focus on IAM *roles*. An IAM role is an IAM identity that you can create in your account that has specific permissions. Unlike an IAM user, A role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.

IAM is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS services by your users. Detailed information about AWS IAM can be found in the documentation.

AWS Lambda

AWS Lambda lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume - there is no charge when your code is not running.

Because your code is only running on-demand, in order to troubleshoot, you'll need to take advantage of monitoring. You can troubleshoot Lambda with Amazon Cloudwatch and also troubleshoot Lambda with AWS X-Ray.

With Lambda, there are 2 types of permissions to be aware of. First, your code running in a Lambda function is granted permissions by using an IAM Role. Second, the service triggering your Lambda function can be granted the permissions to do so with a Lambda Function Policy. When configuring triggers using the AWS Management Console, the console will create the necessary Lambda Function Policy for you when you enable the trigger.

If you want more details about what's available to your code as it runs inside AWS Lambda, you can find out more about the Lambda execution environment in the documentation.