AWS DESCRIBES RESOURCES USED IN THE COCUS DEVOPS CHALLENGE

By Gutemberg Medeiros (gmedeiros@gmail.com)

- IAM
    - Users groups:
      It is a collection of IAM users. User groups let you specify permissions for multiple users, making it easier to manage the permissions for those users.
    - User roles:
      It is an IAM identity that you can create in your account that has specific permissions. For example, FrontEnd develops in the QA squad.
    - IAM Policy:
      It is attached to an IAM user, group, or role. These policies let you specify what that identity can do (its permissions) in the EC2 *runInstances* action for example.

- VPN
    - Endpoint:
      Is the resource created and configured to enable and manage client VPN sessions.
    - Gateway:
      It specifies a virtual private gateway, which is the endpoint on the VPC side of your VPN connection.

- CloudWatch
    - LOG Metric filter:
      It defines the terms and patterns to look for in log data as it is sent to CloudWatch Logs. Then, we use these metric filters to turn log data into numerical CloudWatch metrics that we can graph or set an alarm on.

- Route53
    - Zones:
      It can monitor your public-hosted zones by using Amazon CloudWatch to collect and process raw data into readable, near real-time metrics, plotting that in the CloudWatch Dashboard.

- EC2
    - Instances:
      Based on the on-premises description, I used the simple EC2 instance em two different availability zones to provide redundancy.
    - EBS:
      Use Amazon EBS encryption as a straight-forward encryption solution to guarantee security *at-rest.*

- VPC
    - Private subnet:
      This scenario enables us to run a multi-tiered application with a scalable web front end in a public subnet, and to house our data in a private subnet that is connected to your network by an IPsec AWS Site-to-Site VPN connection.
    - Internet Gateway:
      This internet gateway applied in this can serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for the web instances.
    - Security group:
      I choose this VPC *security group* to act as a virtual firewall, controlling the traffic that is allowed to reach and leave the resources that it is associated with.

- Application Load Balancer
    - LB Listener:
      I choose this to automatically distributes incoming traffic across multiple targets, such as EC2 instances, Lambda functions, and apllications. Like an HTTP or HTTPS listener connection request.
    - Target group:
      It’s used to route requests to one or more registered targets.

- LAMBDA
    - Application
      Used by deploying the APP application.
    - Function

- RDS
    - MySQL Replication

      I used read replicas to configure replication between *eu-central-1a* zone, and *eu-central-1c* zone RDS MySQL instances for redundancy.

- KMS

  I choose to use in this case to encrypt Amazon RDS primary instance, and both RDS read instances too. Include all logs, backups, and snapshots using the same KMS key as the primary MySQL instance.

- S3 Bucket

  I used Apache Airflow plugin to store the apache logs in the S3 bucket, running in the booth EC2 instances.