Tutorials Dojo – Practice Exam – Review Mode – 2

**Final Results 66.7% (44/65) – 05/25/2023**

**Services to Review**

ECS Batch Processing

* Leverages S3, SQS, and ECS
* Docker containers are particularly suited for batch job workloads. Batch jobs are often short-lived and embarrassingly parallel. You can package your batch processing application into a Docker image so that you can deploy it anywhere, such as in an Amazon ECS task.
* Amazon ECS supports batch jobs. You can use Amazon ECS Run Task action to run one or more tasks once. The Run Task action starts the ECSDocker containers are particularly suited for batch job workloads. Batch jobs are often short-lived and embarrassingly parallel. You can package your batch processing application into a Docker image so that you can deploy it anywhere, such as in an Amazon ECS task.
* Amazon ECS supports batch jobs. You can use Amazon ECS *Run Task* action to run one or more tasks once. The Run Task action starts the ECS task on an instance that meets the task’s requirements including CPU, memory, and ports.
* A screenshot of a computer

  Description automatically generated with low confidence
* For example, you can set up an ECS Batch architecture for an image processing application. You can set up an AWS CloudFormation template that creates an Amazon S3 bucket, an Amazon SQS queue, an Amazon CloudWatch alarm, an ECS cluster, and an ECS task definition. Objects uploaded to the input S3 bucket trigger an event that sends object details to the SQS queue. The ECS task deploys a Docker container that reads from that queue, parses the message containing the object name and then downloads the object. Once transformed it will upload the objects to the S3 output bucket.
* By using the SQS queue as the location for all object details, you can take advantage of its scalability and reliability as the queue will automatically scale based on the incoming messages and message retention can be configured. The ECS Cluster will then be able to scale services up or down based on the number of messages in the queue.
* You have to create an IAM Role that the ECS task assumes in order to get access to the S3 buckets and SQS queue. Note that the permissions of the IAM role don’t specify the S3 bucket ARN for the incoming bucket. This is to avoid a circular dependency issue in the CloudFormation template. You should always make sure to assign the least amount of privileges needed to an IAM role.

SQS

* Message retention period
  + Default 4 days
  + Can be configured for 1 minute to 14 days
  + Once the message retention limit is reached, the messages are automatically deleted
* A single Amazon SQS message queue can contain an unlimited number of messages
  + Standard Queue – 120,000 limit for the number of inflight messages
  + FIFO Queue – 20,000 limit for the number of inflight messages
  + Note – Messages are considered “inflight” after they have been received from the queue by a consuming component, but have not yet been deleted from the queue

Lambda –

* **AWS Lambda** supports the synchronous and asynchronous invocation of a Lambda function. You can control the invocation type only when you invoke a Lambda function. When you use an AWS service as a trigger, the invocation type is predetermined for each service. You have no control over the invocation type that these event sources use when they invoke your Lambda function. Since processing only takes 5 minutes, Lambda is also a cost-effective choice.

A picture containing text, font, screenshot, design

Description automatically generated

* You can use an AWS Lambda function to process messages in an Amazon Simple Queue Service (Amazon SQS) queue. Lambda event source mappings support standard queues and first-in, first-out (FIFO) queues. With Amazon SQS, you can offload tasks from one component of your application by sending them to a queue and processing them asynchronously.
* Kinesis Data Streams is a real-time data streaming service that requires the provisioning of shards. Amazon SQS is a cheaper option because you only pay for what you use. Since there is no requirement for real-time processing in the scenario given, replacing Kinesis Data Streams with Amazon SQS would save more costs.

EKS –

* Amazon EKS Provisions and scales the Kubernetes control plane, including the API servers and backend persistence layer, across multiple AWS AZ’s for high availability and fault tolerance.
* Amazon EKS automatically detects and replaces unhealthy control plane nodes and provides patching for the control plane.
* Amazon EKS is integrated with many AWS services to provide scalability and security for your applications.
  + ELB for load distribution
  + IAM for authentication
  + VPC for isolation
  + CloudTrail for logging

CloudFront –

* CDN that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer friendly environment.
* Integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other services.
  + AWS Shield for DDoS Mitigation
  + Amazon S3
  + ELB or EC2 as origins for apps
  + Lambda@Edge to run custom code closer to customers users and to customize the user experience.
  + Note – if you use AWS origins such as S3, EC2, or ELB – you don’t pay for any data transferred between these services and CloudFront

VPC Peering + Direct Connect + VPN

* In this scenario, you have two VPCs which have peering connections with each other. Note that a VPC peering connection does not support edge to edge routing. This means that if either VPC in a peering relationship has one of the following connections, you cannot extend the peering relationship to that connection:
  + A VPN connection or an AWS Direct Connect connection to a corporate network
  + An Internet connection through an Internet gateway
  + An Internet connection in a private subnet through a NAT device
  + A gateway VPC endpoint to an AWS service; for example, an endpoint to Amazon S3.
  + (IPv6) A ClassicLink connection. You can enable IPv4 communication between a linked EC2-Classic instance and instances in a VPC on the other side of a VPC peering connection. However, IPv6 is not supported in EC2-Classic, so you cannot extend this connection for IPv6 communication.

A picture containing text, screenshot, diagram, font

Description automatically generated

* For example, if VPC A and VPC B are peered, and VPC A has any of these connections, then instances in VPC B cannot use the connection to access resources on the other side of the connection. Similarly, resources on the other side of a connection cannot use the connection to access VPC B.
* Hence, this means that you cannot use VPC-2 to extend the peering relationship that exists between VPC-1 and the on-premises network. For example, traffic from the corporate network can’t directly access VPC-1 by using the VPN connection or the AWS Direct Connect connection to VPC-2

AWS Proton

* AWS Proton allows you to deploy any serverless or container-based application with increased efficiency, consistency, and control. You can define infrastructure standards and continuous delivery pipelines for your organization. Proton breaks down the infrastructure into environment and service (IaC templates)
* Select a standardized service template that AWS Proton uses to create a service that deploys and manages your application in a server instance.
* An AWS Proton Service is an instantiation of a service template, which normally includes several service instances and a pipeline
* With a Component, developers can add supplemental resources to their application, above and beyond what administrators defined in environment and service templates. The developer attaches the component to a service instance.
* AWS Proton provisions infrastructure resources defined by the component just like it provisions resources for environments and service instances

Amazon Data Lifecycle Manager (DLM)

* You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes. Automating snapshot management helps you to:
  + Protect valuable data by enforcing a regular backup schedule.
  + Retain backups as required by auditors or internal compliance.
  + Reduce storage costs by deleting outdated backups.
  + Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon DLM provides a complete backup solution for EBS volumes at no additional cost.

Amazon SQS + SWF

* Simple Queue Service + Simple Workflow Service –
  + SQS offers reliable, highly-scalable hosted queues for storing messages while they travel between applications or microservices. SQS lets you move data between distributed application components and helps you decouple these components.
  + SWF is a web service that makes it easy to coordinate work across distributed application components.

AWS Config

* AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.
* Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.
* You can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine overall compliance against the configurations specified in the internal guidelines
* Simplify compliance auditing, security analysis, change management, and troubleshooting
* Config Rules –
  + Enforce ideal configuration
  + Checks if the applied configuration of resourced violate any conditions in the rule
* Config Dashboard shows the compliance status of rules and resources

Amazon Route 53 + ELB

* To route domain traffic to an ELB load balancer, use Amazon Route 53 to create an alias record that points to your load balancer. An alias record is a Route 53 extension to DNS. It’s similar to a CNAME record, but you can create an alias record both for the root domain, such as tutorialsdojo.com and for subdomains, such as portal.tutorialsdojo.com. (You can create CNAME records only for subdomains.) To enable IPv6 resolution, you would need to create a second resource record, tutorialsdojo.com ALIAS AAAA -> myelb.us-west-2.elb.amazonnaws.com, this is assuming your Elastic Load Balancer has IPv6 support.

AWS DataSync

* Allows you to copy large datasets with millions of files without having to build custom solutions with open source tools or licenses and manage expensive commercial network acceleration software
* You can use DataSync to migrate active data to AWS, transfer data to the cloud for analysis and processing, archive data to free up on-premises storage capacity, or replicate data to AWS for business continuity
* AWS DataSync enables you to migrate you on-premises data to
  + S3
  + EFS
  + FSx for Windows File Server
* You can configure DataSync to make an initial copy of your entire dataset and schedule subsequent incremental transfers of changing data towards Amazon S3
* AWS DataSync is primarily used to migrate existing data to Amazon S3. On the other hand, AWS Storage Gateway is more suitable if you still want to retain access to the migrated data and for ongoing updates from your on-premises file-based applications
* DatSync can transfer hundreds of terabytes and millions of files at speeds up to 10x faster than open-source tools
  + Over the internet
  + AWS Direct Connect
* Steps
  + Deploy the DataSync Agent
  + Connect it to your file system
  + Select your AWS storage resources
  + Start moving data between them
    - Note – you pay only for data you move
* AWS DataSync – Migration / Move
* AWS Storage Gateway – Integration / Replicate

Bastion Host

* Deploy a Windows Bastion Host with an Elastic IP address in the public subnet and allow RDP access to bastion only from the corporate IP Addresses
* A Bastion Host is a special purpose computer on a network specifically designed and configured to withstand attacks. If you have a bastion host in AWS, it is basically just an EC2 Instance. It should be in a public subnet with either a Public or Elastic IP address with sufficient RDP or SSH access defined in the security group. Users log on to the bastion via SSH or RDP and then use that session to manage other hosts in the private subnets.
* Windows Bastion – RDP
* Linux Bastion – SSH

RDS Proxy

* If a “Too Many Connections” error happens to a client connecting to a MySQL database, it means all available connections are in use by other clients. Opening a connection consumes resources on the DB server. Since Lambda Functions can scale to tens of thousands of concurrent connection, your DB needs more resources to open and maintain connections instead of executing queries. The maximum number of connections a DB can support is largely determined by the amount of memory allocated to it. Upgrading to a DB instance with higher memory is a straightforward way of solving the problem. Another approach would be to maintain a connection pool that clients can reuse. – This is where RDS Proxy comes in.
* RDS Proxy helps you manage a large number of connections from Lambda to an RDS DB by establishing a warm connection pool to the DB. Your Lambda Functions interact with RDS Proxy instead of the DB instance. It handles the connection pooling necessary for scaling many simultaneous connections created by concurrent Lambda Functions. This allows your Lambda applications to reuse existing connections, rather than creating new connections for every function invocation.

CloudWatch + SNS

* You can use Amazon CloudWatch to monitor the DB and then SNS to send the emails to the operations team. Take note that you should use SNS instead of SES (Simple Email Service) when you want to monitor your EC2 instances.
* CloudWatch collects monitoring and operating data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS, and on-premises servers.
* SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

AWS Snowball Edge

* A type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can undertake local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud.
* Each Snowball Edge device can transport data at speeds faster than the internet. This transport is done by shipping the data in the appliances through a regional carrier. The appliances are rugged shipping containers, complete with E Ink shipping labels. The AWS Snowball Edge device differs from the Standard Snowball because it can bring the power of the AWS Cloud to your on-premises location, with local storage and compute functionality.
* Snowball Edge devices have three options for device configurations
  + Storage Optimized
  + Compute Optimized
  + With GPU