Exam Three Notes

Uday Manchanda

September 17, 2021

1 Questions I had no idea/got wrong

1.1 Question 1

- Question
  - The DevOps team at an IT company has created a custom VPC (V1) and attached an Internet Gateway (I1) to the VPC.
  - The team has also created a subnet (S1) in this custom VPC and added a route to this subnet's route table (R1) that directs internet-bound traffic to the Internet Gateway.
  - Now the team launches an EC2 instance (E1) in the subnet S1 and assigns a public IPv4 address to this instance. Next the team also launches a NAT instance (N1) in the subnet S1.
  - Under the given infrastructure setup, which of the following entities is doing the Network Address Translation for the EC2 instance E1?
- Answer: Internet Gateway (I1)
- An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.
- An Internet Gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. Therefore, for instance E1, the Network Address Translation is done by Internet Gateway I1.

1.2 Question 6

- Question
  - A financial services company is migrating their messaging queues from self-managed message-oriented middleware systems to Amazon SQS. The development team at the company wants to minimize the costs of using SQS.

  - As a solutions architect, which of the following options would you recommend for the given use-case?

- Answer: Use SQS long polling to retrieve messages from your Amazon SQS queues
- Amazon SQS provides short polling and long polling to receive messages from a queue. By default, queues use short polling.
- With short polling, Amazon SQS sends the response right away, even if the query found no messages.
- With long polling, Amazon SQS sends a response after it collects at least one available message, up to the maximum number of messages specified in the request. Amazon SQS sends an empty response only if the polling wait time expires.
- Long polling makes it inexpensive to retrieve messages from your Amazon SQS queue as soon as the messages are available. Using long polling can reduce the cost of using SQS because you can reduce the number of empty receives.

1.3 Question 7

- Question
  - A company is looking for an orchestration solution to manage a workflow that uses AWS Glue and Amazon Lambda to process data on its S3 based data lake.
  - As a solutions architect, which of the following AWS services involves the LEAST development effort for this use-case?
- Answer: AWS Step Functions
- AWS Step Functions lets you coordinate and orchestrate multiple AWS services such as AWS Lambda and AWS Glue into serverless workflows.

1.4 Question 10

- Question
  - A retail company uses AWS Cloud to manage its IT infrastructure.
  - The company has set up "AWS Organizations" to manage several departments running their AWS accounts and using resources such as EC2 instances and RDS databases. The company wants to provide shared and centrally-managed VPCs to all departments using applications that need a high degree of interconnectivity.
  - As a solutions architect, which of the following options would you choose to facilitate this use-case?

- Answer: Use VPC sharing to share one or more subnets with other AWS accounts belonging to the same parent organization from AWS Organizations
- VPC sharing (part of Resource Access Manager) allows multiple AWS accounts to create their application resources such as EC2 instances, RDS databases, Redshift clusters, and Lambda functions, into shared and centrally-managed Amazon Virtual Private Clouds (VPCs).
- To set this up, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations.

1.5 Question 11

- Question
  - A company has a hybrid cloud structure for its on-premises data center and AWS Cloud infrastructure. The company wants to build a web log archival solution such that only the most frequently accessed logs are available as cached data locally while backing up all logs on Amazon S3.
  - As a solutions architect, which of the following solutions would you recommend for this use-case?
- Answer: Use AWS Volume Gateway - Cached Volume - to store the most frequently accessed logs locally for low-latency access while storing the full volume with all logs in its Amazon S3 service bucket
- AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. The service provides three different types of gateways – Tape Gateway, File Gateway, and Volume Gateway – that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access. With cached volumes, the AWS Volume Gateway stores the full volume in its Amazon S3 service bucket, and just the recently accessed data is retained in the gateway's local cache for low-latency access.

1.6 Question 12

- Question
  - A retail company has connected its on-premises data center to the AWS Cloud via AWS Direct Connect. The company wants to be able to resolve DNS queries for any resources in the on-premises network from the AWS VPC and also resolve any DNS queries for resources in the AWS VPC from the on-premises network.
  - As a solutions architect, which of the following solutions can be combined to address the given use case? (Select two)

- Answer: Create an inbound endpoint on Route 53 Resolver and then DNS resolvers on the on-premises network can forward DNS queries to Route 53 Resolver via this endpoint
- Answer: Create an outbound endpoint on Route 53 Resolver and then Route 53 Resolver can conditionally forward queries to resolvers on the on-premises network via this endpoint

1.7 Question 13

- Question
  - A company recently experienced a database outage in its on-premises data center. The company now wants to migrate to a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.
- Answer: Set up an RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data
- When you provision an RDS Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ).

1.8 Question 14

- Question
  - An e-commerce company is planning to migrate their two-tier application from on-premises infrastructure to AWS Cloud.
  - As the engineering team at the company is new to the AWS Cloud, they are planning to use the Amazon VPC console wizard to set up the networking configuration for the two-tier application having public web servers and private database servers.
  - Can you spot the configuration that is NOT supported by the Amazon VPC console wizard?
- Answer: VPC with a public subnet only and AWS Site-to-Site VPN access

1.9 Question 21

- Question
  - The engineering team at a social media company wants to use Amazon CloudWatch alarms to automatically recover EC2 instances if they become impaired. The team has hired you as a solutions architect to provide subject matter expertise.

  - As a solutions architect, which of the following statements would you identify as CORRECT regarding this automatic recovery process? (Select two)

- Answer: If your instance has a public IPv4 address, it retains the public IPv4 address after recovery

- Answer: A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata

1.10 Question 30

- Question
  - A startup has recently moved their monolithic web application to AWS Cloud.
  - The application runs on a single EC2 instance. Currently, the user base is small and the startup does not want to spend effort on elaborate disaster recovery strategies or Auto Scaling Group. The application can afford a maximum downtime of 10 minutes.
  - In case of a failure, which of these options would you suggest as a cost-effective and automatic recovery procedure for the instance?

- Answer: Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance, in case the instance fails. The instance, however, should only be configured with an EBS volume

1.11 Question 33

- Question
  - An e-commerce company uses Microsoft Active Directory to provide users and groups with access to resources on the on-premises infrastructure. The company has extended its IT infrastructure to AWS in the form of a hybrid cloud. The engineering team at the company wants to run directory-aware workloads on AWS for a SQL Server-based application. The team also wants to configure a trust relationship to enable single sign-on (SSO) for its users to access resources in either domain.
  - As a solutions architect, which of the following AWS services would you recommend for this use-case?

- Answer: AWS Managed Microsoft AD

- AWS Directory Service provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory (AD) with other AWS services.

- AWS Directory Service for Microsoft Active Directory (aka AWS Managed Microsoft AD) is powered by an actual Microsoft Windows Server Active Directory (AD), managed by AWS.

1.12 Question 35

- Question
  - An engineering lead is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow EC2 instances to download software updates.
  - Which of the following options represents the correct solution to set up internet access for the private subnets?
- Answer: Set up three NAT gateways, one in each public subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the NAT gateway in its AZ
- You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.

1.13 Question 39

- Question
  - A company wants to migrate its on-premises databases to AWS Cloud.
  - The CTO at the company wants a solution that can handle complex database configurations such as secondary indexes, foreign keys, and stored procedures.
  - As a solutions architect, which of the following AWS services should be combined to handle this use-case? (Select two)
- Answer: AWS Schema Conversion Tool
- Answer: AWS Database Migration Service
- AWS Database Migration Service helps you migrate databases to AWS quickly and securely.
- That makes heterogeneous migrations a two-step process. First use the AWS Schema Conversion Tool to convert the source schema and code to match that of the target database, and then use the AWS Database Migration Service to migrate data from the source database to the target database.

1.14 Question 41

- Question

  - A gaming company uses Application Load Balancers (ALBs) in front of Amazon EC2 instances for different services and microservices.
  - The architecture has now become complex with too many ALBs in multiple AWS Regions. Security updates, firewall configurations, and traffic routing logic have become complex with too many IP addresses and configurations.
  - The company is looking at an easy and effective way to bring down the number of IP addresses allowed by the firewall and easily manage the entire network infrastructure. Which of these options represents an appropriate solution for this requirement?

- Answer: Launch AWS Global Accelerator and create endpoints for all the Regions. Register the ALBs of each Region to the corresponding endpoints

- AWS Global Accelerator is a networking service that sends your user's traffic through Amazon Web Service's global network infrastructure, improving your internet user performance by up to 60

1.15 Question 44

- Question
  - An IT company is looking to move its on-premises infrastructure to AWS Cloud. The company has a portfolio of applications with a few of them using server bound licenses that are valid for the next year. To utilize the licenses, the CTO wants to use dedicated hosts for a one year term and then migrate the given instances to default tenancy thereafter.
  - As a solutions architect, which of the following options would you identify as CORRECT for changing the tenancy of an instance after you have launched it? (Select two)

- Answer: You can change the tenancy of an instance from dedicated to host

- Answer: You can change the tenancy of an instance from host to dedicated

1.16 Question 46

- Question
  - A developer has configured inbound traffic for the relevant ports in both the Security Group of the EC2 instance as well as the Network Access Control List (NACL) of the subnet for the EC2 instance.
  - The developer is, however, unable to connect to the service running on the Amazon EC2 instance.
  - As a solutions architect, how will you fix this issue?

- Answer: Security Groups are stateful, so allowing inbound traffic to the necessary ports enables the connection. Network ACLs are stateless, so you must allow both inbound and outbound traffic

1.17 Question 48

- Question
  - A video conferencing application is hosted on a fleet of EC2 instances which are part of an Auto Scaling group (ASG).
  - The ASG uses a Launch Configuration (LC1) with "dedicated" instance placement tenancy
  - but the VPC (V1) used by the Launch Configuration LC1 has the instance tenancy set to default.
  - Later the DevOps team creates a new Launch Configuration (LC2) with "default" instance placement tenancy
  - but the VPC (V2) used by the Launch Configuration LC2 has the instance tenancy set to dedicated.
  - Which of the following is correct regarding the instances launched via Launch Configuration LC1 and Launch Configuration LC2?
- Answer: The instances launched by both Launch Configuration LC1 and Launch Configuration LC2 will have dedicated instance tenancy
- When you create a launch configuration, the default value for the instance placement tenancy is null and the instance tenancy is controlled by the tenancy attribute of the VPC.

1.18 Question 52

- Question
  - A company has set up "AWS Organizations" to manage several departments running their own AWS accounts.
  - The departments operate from different countries and are spread across various AWS Regions.
  - The company wants to set up a consistent resource provisioning process across departments so that each resource follows pre-defined configurations such as using a specific type of EC2 instances, specific IAM roles for Lambda functions, etc.
  - As a solutions architect, which of the following options would you recommend for this use-case?
- Answer: Use AWS CloudFormation StackSets to deploy the same template across AWS accounts and regions

- AWS CloudFormation StackSet extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation.

1.19 Question 55

- Question
  - An AWS Organization is using Service Control Policies (SCP) for central control over the maximum available permissions for all accounts in their organization.
  - This allows the organization to ensure that all accounts stay within the organization's access control guidelines.
  - Which of the given scenarios are correct regarding the permissions described below? (Select three)
- Answer: If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable SCPs, the user or role can't perform that action
- Answer: SCPs affect all users and roles in attached accounts, including the root user
- Answer: SCPs do not affect service-linked role

1.20 Question 56

- Question
  - The DevOps team at an IT company is provisioning a two-tier application in a VPC with a public subnet and a private subnet.
  - The team wants to use either a NAT instance or a NAT gateway in the public subnet to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet
  - but needs some technical assistance in terms of the configuration options available for the NAT instance and the NAT gateway.
  - As a solutions architect, which of the following options would you identify as CORRECT? (Select three)
- Answer: NAT instance can be used as a bastion server
- Answer: Security Groups can be associated with a NAT instance
- Answer: NAT instance supports port forwarding
- A NAT instance or a NAT Gateway can be used in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet.

1.21 Question 60

- Question
  - The development team at a retail company wants to optimize the cost of EC2 instances. The team wants to move certain nightly batch jobs to spot instances. The team has hired you as a solutions architect to provide the initial guidance.
  - Which of the following would you identify as CORRECT regarding the capabilities of spot instances? (Select three)
- Answer: If a spot request is persistent, then it is opened again after your Spot Instance is interrupted
- Answer: Spot blocks are designed not to be interrupted
- Answer: When you cancel an active spot request, it does not terminate the associated instance

1.22 Question 65

- Question
  - A company has its application servers in the public subnet that connect to the RDS instances in the private subnet. For regular maintenance, the RDS instances need patch fixes that need to be downloaded from the internet.
  - Considering the company uses only IPv4 addressing and is looking for a fully managed service, which of the following would you suggest as an optimal solution?
- Answer: Configure a NAT Gateway in the public subnet of the VPC
- You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.

1.23 Question 15

- Question
  - A data analytics company is using SQS queues for decoupling the various processes of an application workflow. The company wants to postpone the delivery of certain messages to the queue by one minute while all other messages need to be delivered immediately to the queue.
  - As a solutions architect, which of the following solutions would you suggest to the company?

- Answer: Use message timers to postpone the delivery of certain messages to the queue by one minute
- You can use message timers to set an initial invisibility period for a message added to a queue.

1.24 Question 17

- Question
  - The engineering team at a company wants to use Amazon SQS to decouple components of the underlying application architecture. However, the team is concerned about the VPC-bound components accessing SQS over the public internet.
  - As a solutions architect, which of the following solutions would you recommend to address this use-case?
- Answer: Use VPC endpoint to access Amazon SQS
-

1.25 Question 22

- Question
  -
- Answer:

1.26 Question 24

- Question
  - A media company has its corporate headquarters in Los Angeles with an on-premises data center using an AWS Direct Connect connection to the AWS VPC. The branch offices in San Francisco and Miami use Site-to-Site VPN connections to connect to the AWS VPC. The company is looking for a solution to have the branch offices send and receive data with each other as well as with their corporate headquarters.
  - As a solutions architect, which of the following AWS services would you recommend addressing this use-case?
- Answer: VPN CloudHub
- If you have multiple AWS Site-to-Site VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub.

1.27 Question 31

- Question
  - A health care application processes the real-time health data of the patients into an analytics workflow. With a sharp increase in the number of users, the system has become slow and sometimes even unresponsive as it does not have a retry mechanism. The startup is looking at a scalable solution that has minimal implementation overhead.
  - Which of the following would you recommend as a scalable alternative to the current solution?
- Answer: Use Amazon Kinesis Data Streams to ingest the data, process it using AWS Lambda or run analytics using Kinesis Data Analytics

1.28 Question 32

- Question
  - A media startup is looking at hosting their web application on AWS Cloud. The application will be accessed by users from different geographic regions of the world. The main feature of the application requires the upload and download of video files that can reach a maximum size of 10GB. The startup wants the solution to be cost-effective and scalable with the lowest possible latency for a great user experience.
- Answer: Use Amazon S3 for hosting the web application and use S3 Transfer Acceleration to reduce the latency that geographically dispersed users might face
- Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500 percent for long-distance transfer of larger objects.

1.29 Question 45

- Question
  - An e-commerce company runs its web application on EC2 instances in an Auto Scaling group and it's configured to handle consumer orders in an SQS queue for downstream processing. The DevOps team has observed that the performance of the application goes down in case of a sudden spike in orders received.
  - As a solutions architect, which of the following solutions would you recommend to address this use-case?
- Answer: Use a target tracking scaling policy based on a custom Amazon SQS queue metric

- If you use a target tracking scaling policy based on a custom Amazon SQS queue metric, dynamic scaling can adjust to the demand curve of your application more effectively.

1.30 Question 47

- Question
  - The engineering team at an e-commerce company wants to migrate from SQS Standard queues to FIFO queues with batching.
- Answer: Delete the existing standard queue and recreate it as a FIFO queue
- Make sure that the name of the FIFO queue ends with the .fifo suffix
- Make sure that the throughput for the target FIFO queue does not exceed 3,000 messages per second

1.31 Question 57

- Question
  - A retail organization is moving some of its on-premises data to AWS Cloud. The DevOps team at the organization has set up an AWS Managed IPSec VPN Connection between their remote on-premises network and their Amazon VPC over the internet.
  - Which of the following represents the correct configuration for the IPSec VPN Connection?
- Answer: Create a Virtual Private Gateway on the AWS side of the VPN and a Customer Gateway on the on-premises side of the VPN
- Amazon VPC provides the facility to create an IPsec VPN connection (also known as site-to-site VPN) between remote customer networks and their Amazon VPC over the internet.

1.32 Question 61

- Question
  - The DevOps team at an IT company has recently migrated to AWS and they are configuring security groups for their two-tier application with public web servers and private database servers. The team wants to understand the allowed configuration options for an inbound rule for a security group.
  - As a solutions architect, which of the following would you identify as an INVALID option for setting up such a configuration?
- Answer: You can use an Internet Gateway ID as the custom source for the inbound rule

1.33 Question 62

- Question
  - A financial services company wants to move the Windows file server clusters out of their datacenters. They are looking for cloud file storage offerings that provide full Windows compatibility. Can you identify the AWS storage services that provide highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol compatible with Windows systems? (Select two)
- Answer: Amazon FSx for Windows File Server
- Answer: File Gateway Configuration of AWS Storage Gateway
- Storage Gateway provides 3 types of storage interfaces for on-premises applications: File, Volume, and Tape. The File Gateway enables you to store and retrieve objects in Amazon S3 using file protocols such as Network File System (NFS) and Server Message Block (SMB).

1.34 Question 63

- Question
  - Your application is hosted by a provider on yourapp.provider.com. You would like to have your users access your application using www.your-domain.com, which you own and manage under Route 53.
  - What Route 53 record should you create?
- Answer: CNAME record
- A CNAME record maps DNS queries for the name of the current record, such as acme.example.com, to another domain (example.com or example.net) or subdomain (acme.example.com or zenith.example.org).
- For example, if you register the DNS name example.com, the zone apex is example.com. You cannot create a CNAME record for example.com, but you can create CNAME records for www.example.com, newproduct.example.com, and so on.

1.35 Question 64

- Question
  - The business analytics team at a company has been running ad-hoc queries on Oracle and PostgreSQL services on Amazon RDS to prepare daily reports for senior management. To facilitate the business analytics reporting, the engineering team now wants to continuously replicate this data and consolidate these databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift.

  - As a solutions architect, which of the following would you recommend as the MOST resource-efficient solution that requires the LEAST amount of development time without the need to manage the underlying infrastructure?

- Answer: Use AWS Database Migration Service to replicate the data from the databases into Amazon Redshift
- AWS Database Migration Service helps you migrate databases to AWS quickly and securely.

2 Other things to keep in mind

- AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS
- By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection, and configuring routing to pass traffic through the connection.
- Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3.
- Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.
- VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
- VPC sharing allows customers to share subnets with other AWS accounts within the same AWS Organization.
- AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.
- An Elastic Fabric Adapter (EFA) is a network device that you can attach to your Amazon EC2 instance to accelerate High Performance Computing (HPC) and machine learning applications.
- AWS Global Accelerator is a networking service that helps you improve the availability and performance of the applications that you offer to your global users.
- To ensure that an Elastic Load Balancer stops sending requests to instances that are de-registering or unhealthy while keeping the existing connections open, use connection draining.

- You can copy an AMI across AWS Regions
- You can share an AMI with another AWS account
- Copying an AMI backed by an encrypted snapshot cannot result in an unencrypted target snapshot
- Amazon EC2 Auto Scaling chooses the policy that provides the largest capacity, so policy with the custom metric is triggered
- Horizontal scaling: in/out
- Vertical scaling: up/down
- After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance.
- Traffic is routed to instances using the primary **private** IP address specified in the primary network interface for the instance
- The following are the key concepts for a site-to-site VPN:
  - Virtual private gateway: A Virtual Private Gateway (also known as a VPN Gateway) is the endpoint on the AWS VPC side of your VPN connection.
  - VPN connection: A secure connection between your on-premises equipment and your VPCs.
  - VPN tunnel: An encrypted link where data can pass from the customer network to or from AWS.
  - Customer Gateway: An AWS resource that provides information to AWS about your Customer Gateway device.
  - Customer Gateway device: A physical device or software application on the customer side of the Site-to-Site VPN connection.
- Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances.