SET A

1. Amazon EC2 and Resizing Instances

Question: You have deployed a web application on an Amazon EC2 instance using a t2.micro instance type for testing. After launch, you realize that the application needs more compute and memory. Which of the following steps will you take to address this requirement with minimal downtime?

A. Stop the instance, change the instance type to a bigger one, and restart.
B. Modify the instance type in-place from the AWS Management Console while it is running.
C. Launch a new Amazon EC2 instance of a larger size and transfer the Elastic IP from the old instance.
D. Create an Amazon Machine Image (AMI) from the current instance, then launch a bigger instance from that AMI.

Correct Answer: A

Explanation:
To resize an Amazon EC2 instance, you generally need to stop the instance and modify the instance type. Once you update it to the new size, you can start the instance again. This approach preserves the instance's settings, including its instance ID. Option B isn't possible because you cannot change the instance type while it is running. While C and D can also achieve a larger instance, they typically involve more steps or potential configuration changes, making A the most straightforward approach with minimal downtime.

---

2. Amazon VPC Networking

Question: You need to connect your on-premises data center to your AWS environment securely over the internet. Which service should you configure to accomplish this?

A. AWS Direct Connect
B. AWS Site-to-Site VPN
C. AWS VPN CloudHub
D. VPC Peering

Correct Answer: B

Explanation:
AWS Site-to-Site VPN creates a secure IPSec tunnel between your VPC and an on-premises

site, transmitting traffic over the internet in encrypted form. AWS Direct Connect (A) provides a dedicated physical connection and does not use the public internet, while VPC Peering (D) is used to connect VPCs within AWS. AWS VPN CloudHub (C) is used in multi-site scenarios when you have multiple VPN connections.

---

3. Amazon S3 Storage Class

Question: You are storing large amounts of data in Amazon S3 that you rarely access, but you need to ensure that the data is still immediately retrievable when necessary. Which S3 storage class offers the cheapest cost for infrequent access while still allowing instant access?

A. S3 Standard
B. S3 Standard-Infrequent Access (Standard-IA)
C. S3 Glacier Flexible Retrieval (Glacier)
D. S3 Glacier Deep Archive

Correct Answer: B

Explanation:
S3 Standard-Infrequent Access (Standard-IA) is designed for data that is accessed less frequently but requires rapid access when needed. It offers lower storage costs than S3 Standard with a retrieval fee. S3 Glacier and S3 Glacier Deep Archive are intended for archiving, requiring longer retrieval times.

---

4. High Availability with Amazon RDS

Question: You have an Amazon RDS for MySQL instance in a single Availability Zone (AZ). You want to add high availability such that a standby is automatically created in another AZ. Which feature should you enable?

A. Amazon RDS Multi-AZ
B. Amazon RDS Read Replicas
C. Amazon RDS Performance Insights
D. Amazon Aurora Global Database

Correct Answer: A

Explanation:
Amazon RDS Multi-AZ deployments provide a primary database in one Availability Zone and maintain a synchronous standby replica in a different AZ. This setup offers automatic failover in

case of infrastructure failure. Read Replicas (B) are for scaling read-heavy workloads, not for high availability.

---

5. Elastic Load Balancing

Question: Your application is deployed across multiple Amazon EC2 instances behind an Elastic Load Balancer (ELB). You want to ensure that users always return to the same instance once they start a session to avoid losing session data. Which ELB feature would you configure?

A. Cross-zone load balancing
B. Connection draining
C. Sticky sessions
D. Path-based routing

Correct Answer: C

Explanation:
Sticky sessions (also known as session affinity) ensure that all requests from a user during a session are sent to the same target (EC2 instance). This is typically required if stateful session data is stored on local instance memory and not externally (e.g., in a database or cache).

---

6. Serverless Event Handling

Question: You have a serverless application built with AWS Lambda. You want to automatically process new uploads to an S3 bucket. Which of the following must you configure so that your Lambda function runs when an object is created in S3?

A. Enable S3 event notifications on the bucket and configure the Lambda as the event destination.
B. Create a CloudWatch alarm to trigger Lambda whenever a PUT object call is made.
C. Configure an SQS queue and poll it continuously from your Lambda function.
D. Write an AWS Glue job that triggers the Lambda function when new objects appear.

Correct Answer: A

Explanation:
S3 event notifications can be configured to invoke a Lambda function when a specified event (like an object creation) occurs. Options B, C, and D might be used in different scenarios but are not the straightforward method for S3 triggers.

---

7. Security in AWS

Question: Your company wants to give an external data analyst access to certain files stored in an S3 bucket. Which of the following approaches follows AWS best practices for granting limited access?

A. Share your AWS root account credentials so the analyst can access the bucket.
B. Create an AWS Identity and Access Management (IAM) user for the analyst, granting only S3 bucket read access.
C. Set the S3 bucket to “public-read” so the analyst can directly download the files.
D. Use the same IAM credentials as your application, but share the access key privately.

Correct Answer: B

Explanation:
The best practice is to create a dedicated IAM user (or use an IAM role in some cases) with fine-grained permissions to access only the necessary resources. Never share root credentials or set the entire bucket to public unless it’s intentional and risk-assessed.

---

8. Autoscaling Strategy

Question: You have a web application running on a fleet of EC2 instances with an Auto Scaling group. You notice unpredictable spikes in traffic. Which Auto Scaling policy adjustment would best accommodate rapidly changing demand?

A. Scheduled scaling
B. Manual scaling
C. Step scaling based on CPU utilization
D. Enable Reserved Instances

Correct Answer: C

Explanation:
Step scaling (or target tracking scaling) can adjust capacity dynamically based on a metric like CPU utilization. This allows your Auto Scaling group to respond quickly to spikes. Scheduled scaling (A) is useful for predictable, time-based patterns, while manual scaling (B) is the least responsive. Reserved Instances (D) reduce cost but don’t automatically adapt to spikes in traffic.

---

9. Amazon CloudFront Distribution

Question: Your global user base complains of slow downloads of large video files hosted in S3 from regions far from your S3 bucket. Which service do you configure to optimize their download speed?

A. AWS Global Accelerator
B. Amazon Route 53
C. Amazon CloudFront
D. Amazon S3 Transfer Acceleration

Correct Answer: C

Explanation:
Amazon CloudFront is a Content Delivery Network (CDN) that caches content at Edge Locations around the globe, providing faster access to users in different geographic regions. AWS Global Accelerator is typically used for TCP/UDP applications, and Route 53 is DNS. S3 Transfer Acceleration improves data uploads to S3, but CloudFront is designed for large-scale content delivery.

---

10. Infrastructure as Code

Question: You want to provision a repeatable AWS infrastructure setup including VPC, subnets, security groups, and EC2 instances. Which AWS service allows you to define these resources in a template and create them automatically?

A. AWS OpsWorks
B. AWS CodePipeline
C. AWS CodeDeploy
D. AWS CloudFormation

Correct Answer: D

Explanation:
AWS CloudFormation allows you to define your infrastructure in JSON/YAML templates and automatically manage resource creation, updates, and dependencies. OpsWorks (A) is a configuration management service, CodePipeline (B) orchestrates CI/CD workflows, and CodeDeploy (C) automates code deployments

---

SET B

1. Amazon ECS Architecture

Question: You are running an application on Amazon ECS using the Fargate launch type. You need to scale the number of tasks based on CPU and memory usage. Which of the following services should you configure to accomplish this?

A. AWS Budgets
B. Amazon EC2 Auto Scaling
C. AWS Application Auto Scaling
D. AWS OpsWorks

Correct Answer: C

Explanation:
AWS Application Auto Scaling is used to scale ECS (whether Fargate or EC2 launch type), DynamoDB tables, Amazon Aurora replicas, and other services. Amazon EC2 Auto Scaling (B) manages EC2 instances, not ECS tasks. AWS Budgets (A) is related to cost management, and OpsWorks (D) is a configuration management service.

---

2. AWS Shared Responsibility Model

Question: Under the AWS shared responsibility model, which of the following is the customer responsible for?

A. Physical security of data centers
B. Security of the underlying network
C. Patching the guest operating system running on an EC2 instance
D. Maintaining the availability of the AWS global infrastructure

Correct Answer: C

Explanation:
AWS manages the security “of” the cloud (hardware, global infrastructure, etc.), while customers are responsible for security “in” the cloud (patching operating systems, securing data, configuring networks, etc.).

---

3. Amazon CloudTrail

Question: You want to keep track of all the API calls made to your AWS account and store the logs in an S3 bucket for audit purposes. Which service should you enable?

A. Amazon CloudWatch
B. AWS Config
C. AWS Artifact
D. AWS CloudTrail

Correct Answer: D

Explanation:
AWS CloudTrail records AWS API calls and related events in your account, then delivers log files to an Amazon S3 bucket. CloudWatch (A) monitors performance metrics and logs, AWS Config (B) tracks configuration changes, and AWS Artifact (C) is for compliance-related documents.

---

4. Amazon Kinesis Data Stream Scaling

Question: You have a real-time analytics application that consumes data from an Amazon Kinesis data stream. You notice that the shard iterator is being throttled as data volume grows. Which solution helps alleviate this issue?

A. Decrease the shard count
B. Enable Amazon Kinesis Data Firehose
C. Add additional shards to the stream
D. Use Amazon S3 to buffer the data

Correct Answer: C

Explanation:
If you're experiencing throttling due to a high volume of records, you should increase the number of shards in the stream to scale throughput. Decreasing the shard count (A) worsens the problem. Kinesis Data Firehose (B) is a delivery service; it doesn't address shard-level throughput issues directly. Using Amazon S3 (D) does not solve real-time throttling at the ingestion point.

---

5. Amazon EKS and Networking

Question: You plan to run a Kubernetes cluster on AWS using Amazon EKS. You must allow inbound traffic from the internet to some microservices for user-facing APIs. Where should you configure the rule to allow inbound traffic from 0.0.0.0/0 on port 443?

A. Within the EKS VPC routing table
B. In the Security Group associated with the worker nodes or a Load Balancer
C. Within the Kubernetes Ingress rules only
D. In the IAM role assigned to the worker nodes

Correct Answer: B

Explanation:
Traffic must be allowed at the AWS networking layer via Security Groups before it can reach your Kubernetes cluster. While Kubernetes Ingress rules control routing within the cluster, you still need Security Group rules to permit external traffic. IAM roles (D) manage permissions for AWS services, not network traffic.

---

6. NAT Gateway vs. NAT Instance

Question: You have private subnets that need outgoing internet access for updates. You’re considering whether to use a NAT Gateway or NAT Instance. Which of the following is NOT true about NAT Gateways?

A. They scale automatically to accommodate bandwidth requirements.
B. They are managed by AWS, reducing your operational overhead.
C. They can be placed behind an Elastic Load Balancer for high availability.
D. They are created in a specific Availability Zone.

Correct Answer: C

Explanation:
NAT Gateways cannot be placed behind an Elastic Load Balancer. They are managed services that automatically scale (A), are managed by AWS (B), and are created in a single AZ (D). For AZ-level redundancy, you would create multiple NAT Gateways (one per AZ).

---

7. Monitoring AWS Lambda

Question: You have a Lambda function that processes events in near real-time. You need to visualize how many times the function is invoked and track errors over time. Which service provides built-in metrics for Lambda invocations and errors?

A. AWS X-Ray
B. Amazon CloudWatch
C. Amazon CloudTrail
D. Amazon QuickSight

Correct Answer: B

Explanation:
Amazon CloudWatch automatically collects Lambda metrics such as invocations, errors, duration, and throttles. AWS X-Ray (A) provides request tracing and analysis. CloudTrail (C) logs API calls to AWS, while QuickSight (D) is a business intelligence service for data visualization, but not the default metrics store for Lambda.

---

8. Amazon Route 53 Failover Routing

Question: You want to configure DNS failover for a critical application running on EC2 in two different AWS Regions. Which Route 53 routing policy should you set up to redirect traffic to a secondary region if the primary region is unavailable?

A. Weighted Routing
B. Latency Routing
C. Failover Routing
D. Geolocation Routing

Correct Answer: C

Explanation:
Failover Routing allows you to designate a primary and a secondary resource. If health checks fail on the primary, Route 53 directs traffic to the secondary. Weighted routing (A) distributes traffic based on weights, latency routing (B) sends users to the region with the lowest latency, and geolocation routing (D) is based on the user’s location.

---

9. Amazon Aurora Serverless

Question: You need a cost-effective relational database solution for a development workload with highly variable and unpredictable spikes in usage. Which AWS database offering would be most suitable?

A. Amazon RDS for Oracle
B. Amazon DynamoDB
C. Amazon Aurora Serverless
D. Amazon EMR with Hive

Correct Answer: C

Explanation:
Aurora Serverless automatically scales the database capacity up or down based on your application's demands, which is ideal for workloads with unpredictable spikes. RDS for Oracle (A) doesn't scale up or down automatically, DynamoDB (B) is a NoSQL database, and EMR with Hive (D) is more for large-scale data processing.

---

10. Data Encryption on Amazon S3

Question: You need to store sensitive data in S3 and ensure that data is encrypted at rest using keys that are managed by AWS. Which of the following should you use?

A. SSE-S3
B. SSE-C
C. SSE-KMS using a Customer Managed Key
D. Client-side encryption

Correct Answer: A

Explanation:
Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) leverages AES-256 encryption keys managed by AWS. SSE-C (B) uses customer-provided encryption keys. SSE-KMS (C) uses AWS Key Management Service keys, but if you specifically want keys managed entirely by AWS without your own KMS key, SSE-S3 is the best fit. Client-side encryption (D) implies you manage the keys outside of AWS.

SET C

1. Amazon EBS Volume Types

Question: You are designing a high-performance database workload on Amazon EC2. You need an EBS volume type that can deliver high IOPS with consistent low latency. Which EBS volume type is best suited for this requirement?

A. **Throughput Optimized HDD (st1)**
B. **General Purpose SSD (gp3)**
C. **Provisioned IOPS SSD (io2)**
D. **Cold HDD (sc1)**

Correct Answer: C
Explanation:
Provisioned IOPS SSD (io2 or io1) volumes are designed for mission-critical applications that require sustained IOPS performance and low latency. General Purpose SSD (gp3/gp2) is often sufficient for many workloads but may not match the guaranteed performance levels of Provisioned IOPS. Throughput Optimized HDD (st1) and Cold HDD (sc1) are more suitable for sequential throughput-oriented workloads like log processing and are not ideal for high IOPS needs.

---

2. AWS WAF vs. AWS Shield

Question: You want to protect your application running behind an Application Load Balancer from common web exploits like SQL injection and Cross-Site Scripting (XSS). Which AWS service should you enable?

A. **AWS Shield Standard**
B. **AWS Shield Advanced**
C. **AWS WAF (Web Application Firewall)**
D. **Amazon GuardDuty**

Correct Answer: C
Explanation:
AWS WAF (Web Application Firewall) specifically helps you protect web applications from common exploits (e.g., SQL injection, XSS) by allowing you to create custom rules. AWS Shield (Standard or Advanced) protects against DDoS attacks, and GuardDuty is an intelligent threat detection service that monitors for malicious activity in your AWS environment.

---

3. S3 Lifecycle Policies

Question: You have a bucket storing log files. You want these logs to remain in S3 Standard for 30 days, then transition to S3 Glacier Flexible Retrieval for archival, and ultimately delete them after 365 days. Which S3 feature must you configure?

A. **Cross-Region Replication**
B. **Object Versioning**
C. **Lifecycle Configuration**
D. **S3 Batch Operations**

Correct Answer: C
Explanation:
With S3 Lifecycle Configuration, you can set rules to automatically transition objects between storage classes and eventually delete them. Cross-Region Replication (A) copies objects to another bucket in a different region, Versioning (B) stores multiple versions of objects, and S3 Batch Operations (D) allows you to execute bulk actions on large sets of S3 objects.

---

4. Amazon Cognito

Question: You need to implement a secure user sign-up and sign-in experience for a mobile application without managing your own identity backend. Which service should you use?

A. **AWS Identity and Access Management (IAM)**
B. **Amazon Cognito**
C. **AWS Single Sign-On (SSO)**
D. **Amazon GuardDuty**

Correct Answer: B
Explanation:
Amazon Cognito provides user sign-up, sign-in, and access control for web and mobile apps. IAM (A) manages permissions for AWS resources (e.g., EC2, S3) and isn't designed as a direct authentication service for mobile users. AWS SSO (C) is primarily for Single Sign-On across AWS Organizations or SAML apps. GuardDuty (D) is a threat detection service.

---

5. ECS vs. EKS

Question: You want to run containerized applications on AWS and already have substantial Kubernetes expertise. Which container orchestration service is likely the best fit?

A. **Amazon ECS**
B. **AWS Fargate on ECS**
C. **Amazon EKS**
D. **Amazon Elastic Beanstalk**

Correct Answer: C
Explanation:
Amazon EKS (Elastic Kubernetes Service) manages Kubernetes control planes on AWS. If your team has existing Kubernetes expertise, EKS is often a strong choice. ECS (A) is AWS's native container orchestrator without the Kubernetes layer, though it can also be a good fit if you prefer less management overhead of Kubernetes itself. Elastic Beanstalk (D) can run Docker containers but is not a full orchestration platform.

---

6. AWS Database Migration Service (DMS)

Question: You need to migrate data from an on-premises Oracle database to an Amazon RDS for MySQL instance with minimal downtime. Which service is best suited for this task?

A. **AWS Snowball**
B. **AWS Database Migration Service (DMS)**
C. **AWS Storage Gateway**
D. **AWS Backup**

Correct Answer: B
Explanation:
AWS DMS (Database Migration Service) is designed to migrate databases to and from AWS with minimal downtime. Snowball (A) is for physically transferring large amounts of data. Storage Gateway (C) extends on-premises storage into AWS. AWS Backup (D) automates backups of AWS services and on-prem systems but isn't specifically designed for continuous data migration.

---

7. AWS CloudFormation StackSets

Question: Your organization uses multiple AWS accounts, and you want to deploy the same CloudFormation stack (VPCs, IAM roles, etc.) across all these accounts and regions. Which feature do you use?

A. **Nested Stacks**
B. **Change Sets**

C. **AWS CloudFormation StackSets**
D. **AWS CloudFormation Designer**

Correct Answer: C
Explanation:
CloudFormation StackSets enable you to create, update, or delete stacks across multiple AWS accounts and regions with a single operation. Nested Stacks (A) help organize related templates, and Change Sets (B) let you preview changes before applying them. CloudFormation Designer (D) is a visual tool for editing templates.

---

8. S3 Cross-Region Replication

Question: You want to store critical data in an Amazon S3 bucket and automatically replicate it to another bucket in a different region for compliance and disaster recovery. Which feature should you configure?

A. **Versioning**
B. **Multi-Region Access Points**
C. **Cross-Region Replication (CRR)**
D. **Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)**

Correct Answer: C
Explanation:
Cross-Region Replication (CRR) automatically copies S3 objects from one bucket to another in a different region. Versioning (A) must be enabled on the source bucket for CRR, but versioning alone does not replicate data. Multi-Region Access Points (B) route requests across multiple buckets, but that doesn’t replicate your objects. SSE-S3 (D) provides encryption at rest, not replication.

---

9. High-Performance Computing (HPC)

Question: You plan to run HPC workloads requiring low-latency, high-throughput connections between EC2 instances. Which of the following networking features would you configure to optimize HPC cluster performance on AWS?

A. **Enhanced Networking with Elastic Network Adapter (ENA)**
B. **Multiple Internet Gateways**
C. **AWS VPN CloudHub**
D. **Amazon CloudFront**

Correct Answer: A
Explanation:
Enhanced Networking with the Elastic Network Adapter (ENA) or the Intel 82599 Virtual Function (VF) interface provides higher performance (packets per second), lower latency, and lower jitter, which is critical for HPC workloads. Multiple Internet Gateways (B) are not possible per VPC (only one IGW can be attached to a VPC at a time). AWS VPN CloudHub (C) is for site-to-site VPN connectivity, and CloudFront (D) is a CDN, not for HPC internal traffic optimization.

---

10. Amazon Athena vs. QuickSight

Question: You have large amounts of structured and semi-structured data in Amazon S3. You need to run SQL queries directly against this data without loading it into a traditional database. Which AWS service is most appropriate?

A. **Amazon QuickSight**
B. **Amazon Athena**
C. **AWS Glue**
D. **Amazon Redshift**

Correct Answer: B
Explanation:
Amazon Athena is an interactive query service that lets you use standard SQL to analyze data in S3. QuickSight (A) is a BI and reporting tool, not specifically designed to query S3 directly (though it can connect to Athena as a data source). AWS Glue (C) is an ETL service and data catalog; it can be used alongside Athena but is not the querying engine itself. Amazon Redshift (D) would require loading data into a data warehouse.

SET D

1. AWS DataSync vs. AWS Transfer Family

Question: You have a large on-premises NFS file system that needs to be regularly synchronized to an Amazon S3 bucket. Which AWS service is most appropriate for automating and accelerating this process?

A. **AWS Storage Gateway**
B. **AWS DataSync**
C. **AWS Snowmobile**
D. **AWS Transfer Family**

Answer: B

Explanation:
AWS DataSync is designed to automate and accelerate data transfer between on-premises storage (including NFS and SMB shares) and AWS storage services such as Amazon S3, Amazon EFS, or Amazon FSx.

- **AWS Storage Gateway (A)** provides a hybrid cloud storage solution, but it’s typically used to extend or integrate on-premises storage with AWS, not to synchronize an existing file system.
- **AWS Snowmobile (C)** is for extremely large-scale data migrations (exabytes) via a physically transported storage device.
- **AWS Transfer Family (D)** provides SFTP/FTP/FTPS endpoints for transferring files into and out of Amazon S3, not specifically for an NFS sync scenario.

---

2. Amazon EFS vs. Amazon FSx

Question: You need a fully managed shared file system for Linux-based workloads that require the NFS protocol. Which AWS service would you choose?

A. **Amazon EFS**
B. **Amazon FSx for Windows File Server**
C. **Amazon S3**
D. **Amazon FSx for Lustre**

Answer: A

Explanation:
Amazon EFS (Elastic File System) is a serverless, scalable, elastic file system that supports the NFSv4 protocol for Linux-based workloads.

- **FSx for Windows File Server (B)** is a fully managed native Windows file system supporting the SMB protocol.
- **Amazon S3 (C)** is an object storage service, not a file system.
- **FSx for Lustre (D)** is designed for high-performance computing (HPC) and does not provide standard NFS for general-purpose Linux file sharing.

---

3. ECS Networking Mode

Question: You are deploying containerized microservices on Amazon ECS (EC2 launch type) and want each container to have its own IP address directly accessible within your VPC. Which networking mode should you choose?

A. **bridge**
B. **host**
C. **awsvpc**
D. **none**

Answer: C

Explanation:
awsvpc networking mode allows ECS tasks to have the same networking properties as Amazon EC2 instances in the same VPC, giving each task a unique private IP address.

- **bridge (A)** uses Docker's default bridge network, sharing the EC2 instance's network namespace.
- **host (B)** shares the host's network namespace, removing port-mapping constraints but not assigning a unique IP per container.
- **none (D)** disables external networking for the container.

---

4. AWS Budgets vs. AWS Cost Explorer

Question: You want to proactively set alerts if your monthly spending approaches a certain threshold on your AWS account. Which AWS service or feature provides this functionality?

A. **AWS Cost Explorer**
B. **AWS Trusted Advisor**
C. **AWS Budgets**
D. **Amazon QuickSight**

Answer: C

Explanation:
AWS Budgets lets you set custom cost and usage budgets and alerts you when you exceed or approach your thresholds.

- **Cost Explorer (A)** is for analyzing cost and usage trends but doesn't send proactive alerts (though it integrates with Budgets).
- **Trusted Advisor (B)** provides best-practice checks for cost optimization, security, etc., but not budget alerts.

- **Amazon QuickSight (D)** is a BI service for data visualization, not specifically for cost-budget alerts.

---

5. NAT Gateway Cost Optimization

Question: You have multiple private subnets across different Availability Zones (AZs). Each subnet needs outbound internet access for software updates. To minimize costs and provide high availability, how should you deploy your NAT solution?

A. **One NAT Gateway in a single AZ shared by all private subnets**
B. **Multiple NAT Gateways (one per AZ) and route each subnet to the NAT in its own AZ**
C. **Use a NAT Instance in a single AZ with an Elastic IP**
D. **Use an Internet Gateway attached to each private subnet**

Answer: B

Explanation:
For **high availability** and **AZ isolation**, best practice is to deploy **one NAT Gateway per Availability Zone**. Private subnets in each AZ route to the NAT in the same AZ, preventing cross-AZ data transfer costs and avoiding single points of failure.

- A single NAT Gateway for all subnets (A) can become a single point of failure.
- NAT Instances (C) are an older approach and can create performance bottlenecks or scaling issues.
- Private subnets cannot attach an Internet Gateway directly (D)—an IGW must be attached at the VPC level, and routing for private subnets requires a NAT device.

---

6. S3 Multi-Region Access Points

Question: You manage multiple Amazon S3 buckets in different regions. You want a single global endpoint that can automatically route user traffic to the nearest bucket for low latency. Which feature should you configure?

A. **S3 Cross-Region Replication**
B. **S3 Transfer Acceleration**
C. **S3 Multi-Region Access Points**
D. **S3 Bucket Policy**

Answer: C

Explanation:
S3 Multi-Region Access Points provide a single global endpoint that routes S3 requests to the closest available region with your data.

- **Cross-Region Replication (A)** is about copying objects between buckets in different regions, not creating a single global endpoint.
- **Transfer Acceleration (B)** speeds up data uploads and downloads using CloudFront edge locations, but it doesn't route to multiple buckets automatically.
- **S3 Bucket Policy (D)** controls access, not global routing.

---

7. EBS Encryption with SSE-KMS

Question: You want to encrypt data at rest on an Amazon EBS volume using AWS Key Management Service (KMS). What must be done to ensure all new EBS volumes in your account are automatically encrypted by default using your KMS CMK?

A. **Create a default encryption key in IAM**
B. **Turn on EBS default encryption in the Amazon EC2 console and specify your KMS CMK**
C. **Use AWS Certificate Manager to generate an SSL certificate for EBS**
D. **Attach an IAM role to the EC2 instance that references your KMS key**

Answer: B

Explanation:
You can enable **EBS default encryption** in the EC2 console (or via CLI/API) and specify a custom or AWS-managed Customer Master Key (CMK). After enabling, new volumes are automatically encrypted.

- There is no "default encryption key in IAM" (A).
- AWS Certificate Manager (C) is for SSL/TLS certificates, not EBS volume encryption.
- An IAM role (D) alone won't enforce default encryption for all volumes.

---

8. Amazon ECR vs. Public Container Registries

Question: Your organization wants to store and manage Docker images privately within AWS, integrating tightly with IAM and ECS/EKS. Which is the best option?

A. **Upload Docker images to an S3 bucket**
B. **Use Docker Hub for private repositories**

C. **Use Amazon ECR (Elastic Container Registry)**
D. **Use AWS Artifact**

Answer: C

Explanation:
Amazon ECR is a fully managed container registry integrated with AWS IAM for fine-grained permissions and with ECS/EKS for deployment.

- Storing images in S3 (A) doesn't provide the container registry features (tagging, scanning, versioning for containers).
- Docker Hub private repos (B) is external and less tightly integrated with AWS.
- AWS Artifact (D) is for compliance and security documents, not container images.

---

9. AWS Backup vs. Snapshots

Question: You have multiple AWS resources (RDS, EBS, EFS) and want a centralized way to automate and manage backups across all of them. Which service is best suited?

A. **Manual EBS Snapshots**
B. **AWS Backup**
C. **Amazon CloudWatch Events**
D. **AWS Snowball Edge**

Answer: B

Explanation:
AWS Backup provides a centralized service for automating backups across various AWS resources (EBS, RDS, DynamoDB, EFS, etc.).

- Manual EBS snapshots (A) only handle EBS and require manual scheduling or scripts.
- CloudWatch Events (C) can schedule tasks but still requires you to script each backup action.
- Snowball Edge (D) is for offline data transfer, not scheduled backups.

---

10. Multi-Region Database Architecture

Question: You need a globally distributed relational database solution that can handle low-latency reads and quick recovery from a region-wide outage. Which option is best?

A. **Amazon RDS Multi-AZ**
B. **Amazon Aurora Global Database**
C. **Read Replicas in the same AWS Region**
D. **AWS Backup with daily snapshot replication**

Answer: B

Explanation:
Amazon Aurora Global Database replicates data across multiple AWS Regions with sub-second latency and supports fast failover if the primary region becomes unavailable.

- **RDS Multi-AZ (A)** provides high availability within a single region, not across regions.
- **Same-region Read Replicas (C)** do not help with multi-region failover or performance.
- **AWS Backup (D)** is for backups, not active multi-region replication with low-latency reads or quick automated failover.

SET E

1. Amazon Redshift Architecture

Question: You are designing an analytics solution for large-scale, structured data. The solution requires a relational data warehouse with columnar storage and massively parallel processing (MPP). Which service is most appropriate?

A. **Amazon EMR**
B. **Amazon Redshift**
C. **Amazon DynamoDB**
D. **Amazon S3 Select**

Answer: B

Explanation:
Amazon Redshift is a fully managed, petabyte-scale cloud data warehouse with MPP and columnar storage, ideal for complex analytical queries on large datasets.

- **Amazon EMR (A)** provides a managed Hadoop/Spark environment for big data processing (often unstructured or semi-structured).
- **DynamoDB (C)** is a NoSQL key-value database, not a data warehouse.
- **S3 Select (D)** is for querying a subset of data from objects stored in Amazon S3, but it’s not a full-scale data warehousing solution.

---

2. AWS Config vs. CloudTrail

Question: Your organization requires a detailed history of configuration changes to security groups, VPCs, and other AWS resources, along with an ability to track compliance over time. Which service best addresses this need?

A. **AWS CloudTrail**
B. **AWS Config**
C. **Amazon Detective**
D. **Amazon CloudWatch Logs**

Answer: B

Explanation:
AWS Config continuously monitors and records configurations of your AWS resources, allowing you to track configuration changes and assess compliance.

- **CloudTrail (A)** captures API calls and related events but does not provide a resource configuration timeline or compliance checks in the same way as Config.
- **Amazon Detective (C)** helps analyze security data and investigate security findings.
- **CloudWatch Logs (D)** stores log data but requires you to manage your own log ingestion and analysis for configuration history.

---

3. AWS Step Functions vs. Amazon SQS

Question: You want to orchestrate a serverless workflow where multiple Lambda functions run in sequence with conditional branching and error handling. Which service provides a managed state machine for this logic?

A. **Amazon SQS**
B. **Amazon SNS**
C. **AWS Step Functions**
D. **Amazon MQ**

Answer: C

Explanation:
AWS Step Functions is a fully managed workflow service that lets you define state machines for complex orchestration with branching, retries, and parallel execution.

- **Amazon SQS (A)** is a queue service, useful for decoupling components but not designed for complex workflow control.
- **SNS (B)** is a pub/sub messaging service, again not a workflow orchestrator.

- **Amazon MQ (D)** is a managed message broker service for protocols like AMQP and MQTT, also not a workflow engine.

---

4. Amazon Neptune Use Case

Question: You need a fully managed graph database service optimized for highly connected data and queries involving relationships (like social networks or recommendation engines). Which AWS service should you select?

A. **Amazon DynamoDB**
B. **Amazon Neptune**
C. **Amazon DocumentDB (with MongoDB compatibility)**
D. **Amazon Timestream**

Answer: B

Explanation:
Amazon Neptune is a fully managed graph database service that supports both property graph and RDF (Resource Description Framework) models, ideal for use cases such as social networks or knowledge graphs.

- **DynamoDB (A)** is a key-value store.
- **DocumentDB (C)** is a MongoDB-compatible document database.
- **Timestream (D)** is a time-series database for IoT, metrics, and real-time analytics.

---

5. Cross-Account IAM Roles

Question: You have two AWS accounts, **Account A** (data producer) and **Account B** (data consumer). Account B’s application needs to read objects from an S3 bucket owned by Account A. According to AWS best practices, how should you grant access?

A. **Create an IAM user in Account A and share its access key with Account B**
B. **Enable S3 public access on the bucket**
C. **Configure a cross-account IAM role in Account A with trust to Account B**
D. **Use the AWS root account in Account A to generate temporary credentials**

Answer: C

Explanation:
A cross-account IAM role with a trust relationship allows Account B’s principals to assume the role and access the S3 bucket securely.

- Sharing long-term IAM user credentials (A) is an anti-pattern.
- Making the bucket public (B) is not secure.
- Never use the root account (D) or its credentials for routine tasks.

---

6. KMS Customer Managed Keys vs. AWS Managed Keys

Question: You have strict compliance requirements that dictate controlling key rotation and specific key policies for encrypting objects in Amazon S3. Which approach should you use?

A. **Server-Side Encryption with S3-Managed Keys (SSE-S3)**
B. **Client-Side Encryption**
C. **Server-Side Encryption with AWS KMS using AWS-Managed Keys (SSE-KMS)**
D. **Server-Side Encryption with AWS KMS using Customer Managed Keys (SSE-KMS CMK)**

Answer: D

Explanation:
Using **Customer Managed Keys** in KMS (often referred to as CMK) provides fine-grained control over key policies, rotation, and auditing.

- **SSE-S3 (A)** uses keys fully managed by Amazon S3 with less customization.
- **Client-Side Encryption (B)** places the responsibility on the client to encrypt data before uploading.
- **AWS-Managed Keys (C)** are managed by AWS KMS, but you have limited control over policies and rotation schedules compared to customer managed keys.

---

7. AWS Glue Crawler and Data Catalog

Question: You have a data lake in Amazon S3 with diverse file formats (CSV, Parquet, JSON). You need to automatically discover schemas and store them in a central metadata repository. Which service helps accomplish this?

A. **AWS DMS**
B. **AWS Glue**
C. **Amazon QuickSight**
D. **Amazon Athena Workgroups**

Answer: B

Explanation:
AWS Glue can run crawlers on S3 data, detect schemas, and populate the AWS Glue Data Catalog for use by Athena, Redshift Spectrum, and other services.

- **AWS DMS (A)** migrates databases, not designed for discovering data lake schemas.
- **QuickSight (C)** is a BI service, not a schema-discovery solution.
- **Athena Workgroups (D)** isolate query usage and costs, not discover schemas.

---

8. Amazon Elastic Kubernetes Service (EKS) Anywhere

Question: You have an on-premises environment where you want to run containerized workloads on Kubernetes, but still leverage AWS EKS tooling and consistency. Which approach could you consider?

A. **Amazon EKS on AWS Outposts only**
B. **Amazon EKS Anywhere**
C. **Self-managed Kubernetes on EC2**
D. **Amazon Lightsail Containers**

Answer: B

Explanation:
Amazon EKS Anywhere extends EKS to on-premises data centers, providing a consistent Kubernetes experience with AWS tooling and support.

- **EKS on AWS Outposts (A)** requires purchasing Outposts hardware from AWS, which may not be suitable for every on-prem scenario.
- **Self-managed Kubernetes on EC2 (C)** is still within AWS, not on-prem.
- **Amazon Lightsail Containers (D)** is a simplified container platform for small-scale use cases in AWS regions, not on-prem.

---

9. Amazon RDS Read Replica Cross-Region

Question: You have an Amazon RDS MySQL instance in **us-east-1** and want to reduce read latency for users in **eu-west-1**, as well as have a disaster recovery (DR) copy. Which approach is recommended?

A. **Create a Multi-AZ RDS in us-east-1**
B. **Enable cross-region snapshots**

C. **Set up a cross-region Read Replica in eu-west-1**
D. **Use Amazon DynamoDB Global Tables**

Answer: C

Explanation:
Cross-region Read Replicas in RDS allow you to serve read traffic from a region closer to your users and also provide a standby for DR.

- Multi-AZ (A) is within a single region, not cross-region.
- Cross-region snapshots (B) help with backup, not real-time read traffic or immediate DR failover.
- DynamoDB Global Tables (D) are for NoSQL data, not MySQL.

---

10. Reserved Instances vs. Savings Plans

Question: Your organization has a steady-state workload on Amazon EC2 for the next year, and you want to minimize cost while retaining some flexibility in instance family and size. Which purchasing option is most suitable?

A. **Spot Instances**
B. **On-Demand Instances**
C. **Reserved Instances (1-year, All Upfront)**
D. **Compute Savings Plan**

Answer: D

Explanation:
A **Compute Savings Plan** offers cost savings across different instance families, sizes, and regions (even covering AWS Fargate), providing more flexibility than specific Reserved Instances.

- **Spot Instances (A)** are best for fault-tolerant, flexible workloads that can handle interruptions.
- **On-Demand Instances (B)** offer no long-term cost savings.
- **Reserved Instances (C)** provide discounts but are less flexible if your instance needs change.
