**Question 201**

**Difficulty Level: Medium  
Category: Messaging & Analytics**

**A company is developing a marketing communications service for mobile app users. It must send confirmation messages via SMS, receive replies, and store responses for one year.**

**Which solution meets the requirement?**

**A. Use Amazon Connect with Lambda to handle SMS and responses.  
❌ *Incorrect.* Amazon Connect is focused on voice-based interactions, not SMS messaging.**

**B. Use Amazon Pinpoint and configure it to send events to Amazon Kinesis for storage.  
✅ *Correct.* Amazon Pinpoint supports two-way SMS and integrates with Kinesis for stream processing and long-term analytics.**

**C. Use SQS and Lambda to handle SMS flow.  
❌ *Incorrect.* SQS is not built for SMS services.**

**D. Use SNS FIFO with Kinesis.  
❌ *Incorrect.* SNS doesn’t support SMS reply handling.**

**Question 202**

**Difficulty Level:** Simple  
**Category:** Security and Compliance

A company is planning to move its data to an Amazon S3 bucket. The data must be encrypted when it is stored in the S3 bucket. Additionally, the encryption key must be automatically rotated every year.

**Which solution will meet these requirements with the LEAST operational overhead?**

**A.** Move the data to the S3 bucket. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.  
❌ *Incorrect.* SSE-S3 uses AWS-managed keys, which do not support configurable key rotation by the user.

**B.** Create an AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket’s default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.  
✅ *Correct.* This meets encryption and automatic rotation requirements with minimal operational burden.

**C.** Create an AWS Key Management Service (AWS KMS) customer managed key. Set the S3 bucket’s default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket. Manually rotate the KMS key every year.  
❌ *Incorrect.* Manual rotation introduces unnecessary operational overhead.

**D.** Encrypt the data with customer key material before moving the data to the S3 bucket. Create an AWS Key Management Service (AWS KMS) key without key material. Import the customer key material into the KMS key. Enable automatic key rotation.  
❌ *Incorrect.* Imported key material in KMS cannot be automatically rotated.

**Question 203**

**Difficulty Level:** Medium  
**Category:** AWS Technology (Core Services)

The customers of a finance company request appointments with financial advisors by sending text messages. A web application that runs on Amazon EC2 instances accepts the appointment requests. The text messages are published to an Amazon Simple Queue Service (Amazon SQS) queue through the web application. Another application that runs on EC2 instances then sends meeting invitations and meeting confirmation email messages to the customers. After successful scheduling, this application stores the meeting information in an Amazon DynamoDB database.

As the company expands, customers report that their meeting invitations are taking longer to arrive.

**What should a solutions architect recommend to resolve this issue?**

**A.** Add a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database.  
❌ *Incorrect.* DAX only improves read performance. The delay is likely due to processing delays, not read latency.

**Question 204**

**Difficulty Level:** Medium  
**Category:** Cost Optimization

A company needs to perform a data analysis job once a day. The job runs for 30 minutes and must process data stored in S3 using Spark.

**Which solution is MOST cost-effective and operationally efficient?**

**A.** Use Amazon EMR with transient clusters. Submit jobs with AWS Step Functions.  
✅ *Correct.* EMR transient clusters spin up for the job and shut down after, minimizing costs and requiring no persistent resources.

**B.** Use a persistent EMR cluster that runs 24/7.  
❌ *Incorrect.* Costly for an infrequent workload.

**C.** Use an EC2 instance to run Spark manually.  
❌ *Incorrect.* Higher operational overhead and inefficient scaling.

**D.** Use AWS Glue to run the Spark job.  
❌ *Incorrect.* Glue supports Spark, but EMR offers better Spark tuning and scalability.

**Question 205**

**Difficulty Level:** Medium  
**Category:** High Availability

A company runs a public website that must be available even if a full AWS Region goes down.

**What should the solutions architect recommend?**

**A.** Deploy the website across multiple Availability Zones in a single Region.  
❌ *Incorrect.* AZ-level resilience is not sufficient for Region-level outages.

**B.** Use Amazon CloudFront with origins in multiple Regions and Route 53 failover routing.  
✅ *Correct.* CloudFront provides global caching and Route 53 failover ensures automatic redirection in case of a Region failure.

**C.** Use a Regional ALB with Auto Scaling across two AZs.  
❌ *Incorrect.* Still confined to one Region.

**D.** Use AWS Global Accelerator with a single Region.  
❌ *Incorrect.* Global Accelerator improves performance but does not mitigate Region-wide failures alone.

**Question 206**

**Difficulty Level:** Medium  
**Category:** Data Ingestion & Storage

A company collects log data from EC2 instances and needs to analyze it for trends. The solution must be cost-effective and support ad hoc queries.

**What is the BEST solution?**

**A.** Send logs to Amazon S3. Use Amazon Athena to query.  
✅ *Correct.* S3 + Athena allows low-cost storage and flexible, on-demand querying with no infrastructure management.

**B.** Use Amazon Redshift for storage and queries.  
❌ *Incorrect.* Redshift is more expensive and overkill for simple logs.

**C.** Send logs to Amazon DynamoDB.  
❌ *Incorrect.* Not optimal for log analytics or large unstructured datasets.

**D.** Send logs to CloudWatch Logs and use CloudWatch Insights.  
❌ *Incorrect.* Good for real-time monitoring, but not as cost-effective for long-term, large-scale querying.

**Question 207**

**Difficulty Level:** Medium  
**Category:** Serverless & Reliability

A company uses an event-driven application that writes to DynamoDB. During peak loads, DynamoDB write capacity is exceeded and some data is lost.

**What should the solutions architect recommend?**

**A.** Use provisioned DynamoDB and increase write capacity.  
❌ *Incorrect.* Manually increasing capacity may not handle sudden spikes efficiently.

**B.** Switch to on-demand DynamoDB capacity.  
❌ *Incorrect.* May still hit limits during sharp spikes without buffering.

**C.** Use SQS to buffer writes, then use Lambda to write to DynamoDB.  
✅ *Correct.* SQS acts as a buffer and helps absorb spikes, while Lambda handles processing.

**D.** Use Kinesis Firehose to batch writes.  
❌ *Incorrect.* Firehose supports certain destinations, but not direct writes to DynamoDB.

**Question 208**

**Difficulty Level:** Medium  
**Category:** Security & VPC

An EC2 instance in a private subnet needs to access S3 without traversing the internet.

**What is the MOST secure and scalable solution?**

**A.** Use a NAT instance.  
❌ *Incorrect.* NAT instances still send traffic through the internet.

**B.** Use a gateway VPC endpoint for S3.  
✅ *Correct.* Allows secure, private communication with S3 without internet exposure.

**C.** Assign a public IP to the instance.  
❌ *Incorrect.* Breaks the private subnet model and exposes the instance.

**D.** Use an internet gateway and route traffic accordingly.  
❌ *Incorrect.* Insecure and not aligned with private subnet practices.

**Question 209**

**Difficulty Level:** Medium  
**Category:** Compute & Scalability

A web application runs on EC2 instances in multiple AZs behind an ALB. During scale-out, some users lose their session state.

**What is the BEST way to preserve session data during scaling events?**

**A.** Use sticky sessions on the ALB.  
❌ *Incorrect.* Works but can lead to imbalanced load and isn’t scalable.

**B.** Store session data in Amazon ElastiCache.  
✅ *Correct.* ElastiCache (e.g., Redis) provides fast, centralized session storage, ideal for distributed applications.

**C.** Use EC2 instance store volumes for session data.  
❌ *Incorrect.* Data is lost on instance termination and not shared.

**D.** Use instance metadata to store session information.  
❌ *Incorrect.* Not intended for storing user session state.

**Question 210**

**Difficulty Level:** Medium  
**Category:** Application Integration & Scalability

A food delivery service runs on EC2 Auto Scaling groups for both order collection and fulfillment. Fulfillment is slower, and the company needs to ensure no data loss and proper scaling.

**What should the solutions architect do?**

**A.** Use CloudWatch to monitor CPU and scale based on thresholds.  
❌ *Incorrect.* CPU is not the best indicator for asynchronous job queues.

**B.** Use CloudWatch and SNS to trigger new Auto Scaling groups.  
❌ *Incorrect.* Overcomplicated and does not ensure task persistence.

**C.** Use SQS queues for both order collection and fulfillment. Scale based on queue depth.  
✅ *Correct.* Decouples services, buffers tasks, and allows precise scaling.

**D.** Use provisioned concurrency for the EC2 instance.  
❌ *Incorrect.* Provisioned concurrency applies to Lambda, not EC2.

**Question 211**

**Difficulty Level:** Medium  
**Category:** IAM & Security

An external auditor needs temporary, read-only access to all S3 buckets for 1 week. IAM user creation is not permitted.

**What should the solutions architect do?**

**A.** Create an IAM user with read-only S3 access.  
❌ *Incorrect.* IAM user creation is not allowed per the requirements.

**B.** Use Lambda to grant and revoke access after 1 week.  
❌ *Incorrect.* Complex and unnecessary with better native options available.

**C.** Create an IAM role with S3 read-only permissions. Provide temporary credentials using AWS STS.  
✅ *Correct.* STS temporary credentials provide time-limited access securely, without needing user creation.

**D.** Create a service-linked role for read-only access.  
❌ *Incorrect.* Service-linked roles are for AWS services, not external users.

**Question 212**

**Difficulty Level:** Simple  
**Category:** Billing and Pricing

A company needs to export its database once a day to Amazon S3 for other teams to access. The exported object size varies between 2 GB and 5 GB. The S3 access pattern for the data is variable and changes rapidly. The data must be immediately available and must remain accessible for up to 3 months. The company needs the most cost-effective solution that will not increase retrieval time.

**Which S3 storage class should the company use to meet these requirements?**

**A.** S3 Intelligent-Tiering  
✅ *Correct.* S3 Intelligent-Tiering automatically adjusts the storage tier based on usage patterns, offering cost savings without performance compromise.

**B.** S3 Glacier Instant Retrieval  
❌ *Incorrect.* Better suited for archival data; more costly for this use case.

**C.** S3 Standard  
❌ *Incorrect.* Offers instant access but is more expensive over time.

**D.** S3 Standard-Infrequent Access (S3 Standard-IA)  
❌ *Incorrect.* Lower cost, but has retrieval fees and isn't ideal for variable access patterns.

**Question 213**

**Difficulty Level:** Simple  
**Category:** Security and Compliance

A company is developing a new mobile app. The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection. The company has minimal infrastructure and operational staff. The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment.

**What should a solutions architect recommend to meet these requirements?**

**A.** Configure AWS WAF rules and associate them with the ALB.  
✅ *Correct.* AWS WAF protects against common web exploits and is managed by AWS, reducing operational effort.

**B.** Deploy the application using Amazon S3 with public hosting enabled.  
❌ *Incorrect.* This approach exposes the app without adequate protection.

**C.** Deploy AWS Shield Advanced and add the ALB as a protected resource.  
❌ *Incorrect.* AWS Shield protects against DDoS but not application-layer attacks.

**D.** Create a new ALB that directs traffic to an EC2 instance running a third-party firewall.  
❌ *Incorrect.* Increases complexity and operational burden.

**Question 214**

**Difficulty Level:** Medium  
**Category:** Core Services / Data Transformation

A company’s reporting system delivers hundreds of .csv files to an Amazon S3 bucket each day. The company must convert these files to Apache Parquet format and must store the files in a transformed data bucket.

**Which solution will meet these requirements with the LEAST development effort?**

**A.** Use Amazon EMR with Apache Spark to transform and save to S3.  
❌ *Incorrect.* More development and management effort required.

**B.** Use AWS Glue crawler and ETL job to transform the data and write to the transformed bucket.  
✅ *Correct.* Glue offers a fully managed, serverless way to convert data formats with minimal coding.

**C.** Use AWS Batch with Bash scripts to convert and store the data.  
❌ *Incorrect.* Requires more scripting and setup.

**D.** Use AWS Lambda with S3 event notification to trigger transformation.  
❌ *Incorrect.* Not suitable for large file sizes due to Lambda limits.

**Question 215**

**Difficulty Level:** Medium  
**Category:** Storage & Migration

A company has 700 TB of backup data in its on-prem NAS. The data is rarely accessed, but must be retained for 7 years. They have 500 Mbps internet bandwidth and 1 month to complete migration.

**What should a solutions architect do to migrate and store the data at the LOWEST cost?**

**A.** Use AWS Snowball to migrate and then use lifecycle policies to move to S3 Glacier Deep Archive.  
✅ *Correct.* Snowball accelerates bulk transfer, and Glacier Deep Archive offers the lowest storage cost.

**B.** Use a VPN and AWS CLI to upload to Glacier.  
❌ *Incorrect.* Will not meet the migration time window.

**C.** Use Direct Connect to transfer data to S3 and transition to Glacier.  
❌ *Incorrect.* Expensive and not necessary for one-time bulk transfer.

**D.** Use AWS DataSync to transfer data to S3 Glacier.  
❌ *Incorrect.* Over the internet, DataSync would be too slow for this volume.

**Question 216**

**Difficulty Level:** Medium  
**Category:** Security and Networking

A company has an ALB in public subnets targeting EC2 instances in private subnets. Internet traffic is not reaching the instances.

**What should the solutions architect do?**

**A.** Replace the ALB with a Network Load Balancer and add a NAT gateway.  
❌ *Incorrect.* NAT is used for outbound access from private subnets.

**B.** Move EC2 instances to public subnets.  
❌ *Incorrect.* Not recommended for security reasons.

**C.** Update route tables to route 0.0.0.0/0 via the internet gateway from private subnets.  
❌ *Incorrect.* EC2 instances don't need outbound internet access for ALB traffic.

**D.** Place the ALB in public subnets and ensure subnets are associated with the internet gateway.  
✅ *Correct.* ALBs must be in public subnets with correct routing for internet-facing traffic to reach private EC2s.

**Question 217**

**Difficulty Level:** Medium  
**Category:** Compute & Scaling

A web app hosted on EC2 experiences high CPU usage and lag under heavy load. The app must be scalable and handle bursts.

**What is the BEST approach to improve performance and reduce lag?**

**A.** Replace with larger EC2 instance type.  
❌ *Incorrect.* Doesn't scale well for bursty workloads.

**B.** Create Auto Scaling group and scale EC2 based on CPU metrics.  
✅ *Correct.* Auto Scaling adapts to demand and maintains performance.

**C.** Use Lambda instead of EC2.  
❌ *Incorrect.* May require complete re-architecture.

**D.** Add more EC2 instances manually.  
❌ *Incorrect.* Inefficient and not scalable.

**Question 218**

**Difficulty Level:** Simple  
**Category:** Security & Networking

An EC2 web server in a public subnet is not accessible on port 443. The default security group is attached, and network ACLs are blocking all traffic.

**Which steps are required to fix this? (Choose two)**

✅ **A.** Create a security group rule to allow TCP 443 from 0.0.0.0/0  
✅ **E.** Update network ACL to allow inbound TCP 443 and ephemeral outbound ports  
❌ **B.** Security groups don’t use destination-based rules  
❌ **C & D.** ACL rules alone are not sufficient without proper SG settings

**Question 219**

**Difficulty Level:** Medium  
**Category:** Monitoring & Compute Optimization

A stateful EC2 application is showing degraded performance with high memory use. The app runs on M5 instances.

**What should the architect do to resolve this efficiently?**

**A.** Replace with T3 instances in an Auto Scaling group  
❌ *Incorrect.* T3 isn't optimized for memory-intensive workloads.

**B.** Manually increase desired capacity in the Auto Scaling group  
❌ *Incorrect.* Manual scaling is inefficient.

**C.** Replace M5 with R5 instances and monitor built-in memory metrics  
❌ *Incorrect.* EC2 does not provide memory metrics by default.

**D.** Replace M5 with R5 and install CloudWatch Agent for custom memory metrics  
✅ *Correct.* R5 suits memory-heavy apps, and custom metrics provide better monitoring.

**Question 220**

**Difficulty Level:** Simple  
**Category:** Serverless & API Integration

A new API using API Gateway will handle highly variable traffic with asynchronous processing. Several hours may pass without requests.

**What is the MOST cost-effective compute option?**

**A.** AWS Glue  
❌ *Incorrect.* Glue is for ETL, not suitable for APIs.

**B.** AWS Lambda  
✅ *Correct.* Lambda is serverless, scales instantly, and incurs cost only when used.

**C.** Amazon EKS  
❌ *Incorrect.* Adds complexity and cost for sporadic workloads.

**D.** Amazon ECS with EC2  
❌ *Incorrect.* Maintains infrastructure even during idle time.

**Question 221**

**Difficulty Level:** Simple  
**Category:** Billing & Storage

A company must retain EC2 application logs for 7 years and allow concurrent access for analytics.

**What is the MOST cost-effective solution?**

**A.** Amazon EBS  
❌ *Incorrect.* Doesn’t support concurrent access or scale well.

**B.** Amazon EFS  
❌ *Incorrect.* More expensive and overkill for archived logs.

**C.** EC2 instance store  
❌ *Incorrect.* Not persistent or reliable.

**D.** Amazon S3  
✅ *Correct.* S3 offers cost-effective, scalable, concurrent-access storage for long-term retention.

**Question 222**

**Difficulty Level:** Medium  
**Category:** Security and Compliance

A company has hired an external vendor to perform work in the company’s AWS account. The vendor uses an automated tool hosted in its own AWS account and does not have IAM access to the company's account.

**How should a solutions architect grant this access to the vendor?**

**A.** Create an IAM role in the company’s account to delegate access to the vendor’s IAM role. Attach the appropriate IAM policies.  
✅ *Correct.* Cross-account IAM roles securely delegate access between accounts without creating IAM users.

**B.** Create an IAM user in the company’s account with a complex password and attach policies.  
❌ *Incorrect.* IAM users shouldn’t be created for external vendors.

**C.** Create an IAM group and add the vendor’s IAM user to it.  
❌ *Incorrect.* IAM groups can’t include users from other AWS accounts.

**D.** Create a new identity provider with the vendor’s account ID and user name.  
❌ *Incorrect.* Not applicable for AWS-to-AWS account access.

**Question 223**

**Difficulty Level:** Medium  
**Category:** Security and Networking

A company deployed a Java Spring Boot app as a pod on Amazon EKS in private subnets. The app needs to write data to DynamoDB without exposing traffic to the internet.

**What should the solutions architect do? (Choose two)**

✅ **A.** Attach an IAM role with required permissions to the EKS pod  
✅ **D.** Create a VPC endpoint for DynamoDB  
❌ **B.** IAM users are not recommended for pods  
❌ **C.** ACLs don’t control access to AWS services  
❌ **E.** Embedding access keys in code is insecure

**Question 224**

**Difficulty Level:** Simple  
**Category:** Cloud Concepts & Availability

A company rehosted its app to EC2 in a single Region. It now wants to make the app highly available and ensure traffic reaches all EC2 instances randomly.

**What should the company do? (Choose two)**

✅ **C.** Use Route 53 multivalue answer routing  
✅ **E.** Deploy EC2 instances in at least two Availability Zones  
❌ **A & B.** Failover and weighted policies don't ensure random, distributed routing  
❌ **D.** Three instances across two AZs lack optimal fault tolerance

**Question 225**

**Difficulty Level:** Complex  
**Category:** Data Analytics & Ingestion

A media company wants to ingest and analyze petabytes of user activity data, with SQL-based analytics and minimal overhead.

**What’s the BEST solution?**

**A.** Use Kinesis Data Stream delivering to S3  
✅ *Correct.* Supports high availability and integrates well with Athena for on-demand SQL analysis.

**B.** Use Kinesis Firehose delivering to Redshift  
❌ *Incorrect.* Redshift increases management overhead and cost for petabyte-scale ingestion.

**C.** Trigger Lambda from S3 PUT events  
❌ *Incorrect.* Lambda has execution and payload size limitations.

**D.** Use EC2 ingestion service + RDS  
❌ *Incorrect.* High operational overhead and not scalable.

**Question 226**

**Difficulty Level:** Medium  
**Category:** Application Integration & IoT

A company collects data from thousands of remote devices via a REST API on EC2. Device count is expected to grow into the millions.

**What should a solutions architect recommend? (Choose two)**

✅ **A.** Use AWS Glue to process the data in S3  
✅ **B.** Migrate the ingestion layer to Amazon API Gateway + AWS Lambda  
❌ **C.** Use the same EC2 instance and scale vertically  
❌ **D.** Use S3 Lifecycle rules for device filtering  
❌ **E.** Keep EC2 and attach Elastic IPs for consistency

**Question 227**

**Difficulty Level:** Simple  
**Category:** Monitoring & Logging

A company needs to monitor and alert on SSH and RDP access to EC2 instances.

**What should a solutions architect recommend?**

**A.** Use Amazon CloudWatch Logs with metric filters  
✅ *Correct.* VPC Flow Logs + metric filters can detect access patterns and trigger alerts.

**B.** Use AWS Systems Manager Session Manager  
❌ *Incorrect.* Helps manage sessions but not for passive access monitoring.

**C.** Use AWS Config  
❌ *Incorrect.* Tracks config changes, not access attempts.

**D.** Use Amazon EventBridge rules  
❌ *Incorrect.* Doesn’t provide deep traffic inspection.

**Question 228**

**Difficulty Level:** Medium  
**Category:** Security & IAM

A solutions architect must restrict IAM users from launching EC2 instances unless the AMI is approved by the security team.

**What should be done?**

**A.** Use an IAM policy that allows EC2 run instances only with approved AMI IDs  
✅ *Correct.* This provides fine-grained control over which AMIs are permitted.

**B.** Use a service control policy to prevent AMI use  
❌ *Incorrect.* SCPs apply to accounts, not individual users.

**C.** Tag AMIs and deny based on tag  
❌ *Incorrect.* Tag-based deny is not directly enforceable in IAM policies.

**D.** Block EC2 launch access and use only CloudFormation  
❌ *Incorrect.* Overly restrictive and impractical for users.

**Question 229**

**Difficulty Level:** Medium  
**Category:** Serverless & Messaging

A company has a Lambda function that processes messages from an SQS queue. Occasionally, messages are lost during high load.

**What should the solutions architect recommend?**

**A.** Increase SQS visibility timeout  
❌ *Incorrect.* Helps prevent duplicate processing but doesn’t resolve loss under load.

**B.** Add more Lambda concurrency  
✅ *Correct.* Increasing concurrency allows the function to process more messages in parallel.

**C.** Switch to SNS instead of SQS  
❌ *Incorrect.* SNS is for pub-sub, not queueing.

**D.** Set up a dead-letter queue and retry logic  
❌ *Incorrect.* Helps for failed messages, but doesn’t resolve throughput limits.

**Question 230**

**Difficulty Level:** Simple  
**Category:** Cost Optimization

A company wants to analyze logs using Athena. They store logs in S3 and want to minimize costs.

**What is the BEST way to optimize storage costs without affecting analysis?**

**A.** Convert logs to Parquet format  
✅ *Correct.* Parquet reduces query cost and improves performance by storing data in columnar compressed format.

**B.** Use gzip to compress all log files  
❌ *Incorrect.* Compresses files, but doesn’t support columnar analytics.

**C.** Store all logs in Standard S3  
❌ *Incorrect.* Doesn’t reduce Athena query costs.

**D.** Archive old logs in Glacier  
❌ *Incorrect.* Glacier is not queryable by Athena.

**Question 231**

**Difficulty Level:** Medium  
**Category:** Resource Tagging & Inventory

A company wants to identify all components of its application across Regions using the “application” tag.

**What should the solutions architect do?**

**A.** Use AWS CloudTrail  
❌ *Incorrect.* Tracks activity, not tag-based queries.

**B.** Query each AWS service individually using AWS CLI  
❌ *Incorrect.* Time-consuming and inefficient.

**C.** Run a CloudWatch Logs Insights query  
❌ *Incorrect.* Doesn’t provide inventory of resources.

**D.** Use AWS Resource Groups Tag Editor  
✅ *Correct.* Tag Editor allows global search of all tagged resources efficiently.

**Question 232**

**Difficulty Level:** Simple  
**Category:** Security and Compliance

A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company’s operations team needs to be notified when RDP or SSH access to an environment has been established.

**What should a solutions architect recommend?**

**A.** Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.  
❌ *Incorrect.* Application Insights is not used to detect login patterns.

**B.** Configure EC2 with IAM instance profiles using AmazonSSMManagedInstanceCore.  
❌ *Incorrect.* SSM is for remote management but not for detecting access.

**C.** Publish VPC Flow Logs to CloudWatch Logs. Use metric filters and create alarms for RDP/SSH detection.  
✅ *Correct.* VPC Flow Logs combined with CloudWatch can monitor port-level access such as 22/3389 for SSH/RDP.

**D.** Use EventBridge to monitor EC2 instance state changes.  
❌ *Incorrect.* State changes don’t track SSH or RDP connections.

**Question 233**

**Difficulty Level:** Simple  
**Category:** Security and Compliance

A solutions architect has created a new AWS account and must secure the AWS root user access.

**Which two actions should be taken? (Choose two)**

✅ **A.** Ensure the root user uses a strong password.  
✅ **B.** Enable multi-factor authentication (MFA) for the root user.  
❌ **C.** Store root user access keys in an encrypted S3 bucket.  
❌ **D.** Add the root user to a group with administrative permissions.  
❌ **E.** Apply inline policy permissions to the root user.

Root users should not be used routinely and must not have active access keys stored or assigned permissions.

**Question 234**

**Difficulty Level:** Medium  
**Category:** Security and Compliance

A new CRM application will use EC2 with EBS and Aurora. Data must be encrypted both in transit and at rest.

**What is the correct setup?**

**A.** Use KMS certificates for ALB and ACM for EBS/Aurora  
❌ *Incorrect.* ACM cannot encrypt EBS/Aurora storage.

**B.** Use root account and enable encryption for all resources  
❌ *Incorrect.* No global encryption toggle exists.

**C.** Use KMS for EBS and Aurora. Use ACM for ALB TLS.  
✅ *Correct.* This is the correct combination for in-transit (TLS via ACM) and at-rest encryption (via KMS).

**D.** Use BitLocker and import certificates to KMS  
❌ *Incorrect.* BitLocker is not applicable to AWS-native services.

**Question 235**

**Difficulty Level:** Complex  
**Category:** Database Migration

A company is migrating from Oracle to Aurora PostgreSQL. Multiple apps write to the same tables. Migrations are staged with months in between, and data must stay in sync.

**What should a solutions architect recommend?**

**A.** Use AWS DataSync for initial load, then CDC with AWS DMS.  
❌ *Incorrect.* DataSync doesn’t support DB-level CDC.

**B.** Use AWS DMS for full load and CDC.  
❌ *Incorrect.* Lacks schema conversion for Oracle → Aurora PostgreSQL.

**C.** Use AWS SCT with DMS using memory-optimized replication. Create full load + CDC.  
✅ *Correct.* SCT handles schema conversion, and memory-optimized replication helps with heavy workloads.

**D.** Use SCT with compute-optimized instance for CDC of large tables.  
❌ *Incorrect.* Limiting CDC to largest tables may cause data inconsistency.

**Question 236**

**Difficulty Level:** Medium  
**Category:** Application Architecture

A three-tier image-sharing app runs on EC2 instances: frontend, app, and MySQL database. The company needs high availability and scalability with minimal code change.

**What is the BEST solution?**

**A.** Move frontend to S3, use Lambda and DynamoDB.  
❌ *Incorrect.* Requires significant rearchitecture.

**B.** Use Elastic Beanstalk Multi-AZ for all tiers, RDS with read replicas.  
❌ *Incorrect.* Read replicas won’t serve images effectively.

**C.** Host frontend on S3, app layer on EC2 Auto Scaling, DB on memory-optimized EC2.  
❌ *Incorrect.* Still not highly available without DB redundancy.

**D.** Use Elastic Beanstalk for frontend/app, RDS Multi-AZ for DB, and S3 for images.  
✅ *Correct.* Uses managed services, requires few changes, and supports availability.

**Question 237**

**Difficulty Level:** Medium  
**Category:** VPC & Networking

EC2 in VPC-A needs to access files in EC2 in VPC-B (separate accounts) securely and with redundancy.

**What should the network administrator configure?**

**A.** Set up a VPC peering connection between VPC-A and VPC-B  
✅ *Correct.* Simple, secure, no bandwidth bottlenecks, and no single point of failure.

**B.** Set up VPC endpoints  
❌ *Incorrect.* Endpoints are for AWS service access, not EC2-to-EC2 communication.

**C.** Use a virtual private gateway in VPC-B  
❌ *Incorrect.* More suitable for site-to-site VPNs.

**D.** Create private VIF for EC2 in VPC-B  
❌ *Incorrect.* VIFs are for Direct Connect, not EC2 communication.

**Question 238**

**Difficulty Level:** Medium  
**Category:** Billing & Alerts

The company wants to notify engineering accounts if EC2 usage exceeds a monthly threshold.

**What should a solutions architect do?**

**A.** Use AWS Budgets with alert thresholds per account  
✅ *Correct.* AWS Budgets supports per-account usage thresholds with alerting.

**B.** Use Trusted Advisor  
❌ *Incorrect.* Trusted Advisor does not monitor monthly billing limits.

**C.** Use EventBridge to monitor usage  
❌ *Incorrect.* Doesn’t directly track usage thresholds.

**D.** Use Cost Explorer reports  
❌ *Incorrect.* Useful for insights, but not real-time alerting.

**Question 239**

**Difficulty Level:** Simple  
**Category:** Serverless & APIs

A new Go Lambda function must be publicly accessible via HTTPS and use IAM authentication.

**What is the MOST efficient deployment?**

**A.** Use API Gateway and attach IAM auth  
❌ *Incorrect.* Works but requires more setup.

**B.** Use Lambda function URLs with AWS\_IAM auth  
✅ *Correct.* Direct HTTP access with IAM, no additional infra needed.

**C.** Use Lambda@Edge with CloudFront  
❌ *Incorrect.* Overcomplicates the solution.

**D.** Use CloudFront Functions with IAM  
❌ *Incorrect.* CloudFront Functions don’t support IAM auth.

**Question 240**

**Difficulty Level:** Medium  
**Category:** Data Transfer & Cost Optimization

A visualization tool queries a data warehouse over Direct Connect. Queries return ~50 MB each.

**Which solution has the LOWEST egress cost?**

**A.** Host tool on-prem, use internet  
❌ *Incorrect.* High data transfer cost.

**B.** Host tool in AWS, access via internet  
❌ *Incorrect.* Still incurs internet egress.

**C.** On-prem tool + Direct Connect  
❌ *Incorrect.* Still sends large responses out of AWS.

**D.** Host tool in same AWS Region and use Direct Connect  
✅ *Correct.* No egress charges for same-region over Direct Connect.

**Question 241**

**Difficulty Level:** Medium  
**Category:** RDS & Multi-Region Availability

An ed-tech company needs always-on, cross-region PostgreSQL access.

**Which option is most efficient?**

**A.** Host PostgreSQL on EC2  
❌ *Incorrect.* High operational overhead.

**B.** Use RDS Multi-AZ  
❌ *Incorrect.* Multi-AZ is within a single region.

**C.** Use RDS with a cross-region read replica  
✅ *Correct.* Provides cross-region redundancy with minimal management.

**D.** Use snapshots across regions  
❌ *Incorrect.* Snapshots don’t offer real-time access

**Question 242**

**Difficulty Level:** Simple  
**Category:** AWS Technology (Core Services)

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

**Which policy should be used to meet this requirement?**

**A.** Simple routing policy  
❌ *Incorrect.* Simple routing returns only one record.

**B.** Latency routing policy  
❌ *Incorrect.* Returns the lowest-latency instance, not all.

**C.** Multivalue routing policy  
✅ *Correct.* Returns multiple healthy IPs, enabling basic load balancing across healthy instances.

**D.** Geolocation routing policy  
❌ *Incorrect.* Routes based on user's location, not all healthy targets.

**Question 243**

**Difficulty Level:** Medium  
**Category:** AWS Technology (Core Services)

A medical research lab generates study-related data stored in Amazon S3. Clinics across the country need fast access to this data via their on-prem file-based applications.

**What should a solutions architect recommend?**

**A.** Deploy an AWS Storage Gateway file gateway on premises  
✅ *Correct.* File gateway exposes S3 data as SMB/NFS shares compatible with on-prem apps.

**B.** Use AWS DataSync to migrate files to each clinic  
❌ *Incorrect.* Not intended for live, continuous access.

**C.** Use volume gateway at each clinic  
❌ *Incorrect.* Volume gateways are for block storage, not file access.

**D.** Use Amazon EFS  
❌ *Incorrect.* EFS isn’t directly accessible from on-prem without EC2-based solutions.

**Question 244**

**Difficulty Level:** Medium  
**Category:** AWS Technology (Core Services)

A company runs a content management system on a single EC2 instance with both web server and database. They want high availability and scalability.

**What should a solutions architect recommend?**

**A.** Move DB to RDS, create manual EC2 instance and ALB  
❌ *Incorrect.* Manual scaling lacks full availability.

**B.** Use Aurora and EC2 with ALB in same AZ  
❌ *Incorrect.* Single AZ reduces HA.

**C.** Migrate DB to Aurora with read replica in another AZ, create AMI of EC2, use ALB + Auto Scaling across AZs  
✅ *Correct.* Ensures high availability and allows for automated horizontal scaling.

**D.** Move DB to EC2, back up to S3, ALB with Auto Scaling  
❌ *Incorrect.* EC2-hosted DB lacks RDS HA features.

**Question 245**

**Difficulty Level:** Simple  
**Category:** Billing and Pricing

A company launches an app using ALB and EC2 Auto Scaling groups. They require cost-effective deployment of the dev environment.

**What’s the BEST way to reduce dev environment costs?**

**A.** Use only one EC2 in dev  
❌ *Incorrect.* No HA if single instance fails.

**B.** Change ALB algorithm  
❌ *Incorrect.* Doesn't impact instance cost.

**C.** Use smaller instance types  
❌ *Incorrect.* May not reduce cost significantly.

**D.** Reduce max number of EC2s in dev Auto Scaling group  
✅ *Correct.* Maintains scaling capability but limits costs during testing.

**Question 246**

**Difficulty Level:** Medium  
**Category:** AWS Technology (Core Services)

A company runs EC2s in private subnets behind an internet-facing ALB. Internet traffic doesn’t reach the EC2s.

**What’s the fix?**

**A.** Use Network Load Balancer + NAT  
❌ *Incorrect.* NAT is for outbound traffic.

**B.** Move EC2 to public subnets  
❌ *Incorrect.* Violates private subnet design.

**C.** Update route table of private subnets  
❌ *Incorrect.* Internet-facing ALB must be in public subnets.

**D.** Place ALB in public subnets with route to private subnets  
✅ *Correct.* ALB must be internet-facing in public subnets to forward traffic privately.

**Question 247**

**Difficulty Level:** Medium  
**Category:** AWS Technology (Core Services)

A company plans to add an RDS MySQL read replica to handle slow reads.

**What must the solutions architect do first? (Choose two)**

✅ **A.** Enable binary logging on the source DB  
✅ **E.** Enable automated backups  
❌ **B.** Failover priority is irrelevant to replicas  
❌ **C.** Waiting for long transactions is unnecessary  
❌ **D.** Global tables are for DynamoDB.

**Question 248**

**Difficulty Level:** Medium  
**Category:** AWS Technology (Core Services)

Analytics software on EC2 is overloaded (100% CPU). Some data isn’t processed.

**What should a solutions architect do?**

**A.** Add ALB  
❌ *Incorrect.* Doesn’t reduce CPU or queue backlog.

**B.** Use S3 VPC endpoint  
❌ *Incorrect.* Unrelated to CPU utilization.

**C.** Use more powerful EC2 instance  
❌ *Incorrect.* Doesn’t address demand fluctuation.

**D.** Use SQS to queue requests; scale EC2 using Auto Scaling  
✅ *Correct.* This decouples ingestion and allows dynamic scaling.

**Question 249**

**Difficulty Level:** Simple  
**Category:** AWS Technology (Core Services)

A media app hosted in AWS needs shared, fully managed SMB storage.

**What’s the best solution?**

**A.** Storage Gateway with volume share  
❌ *Incorrect.* For hybrid workloads, not fully managed in cloud.

**B.** Storage Gateway tape gateway  
❌ *Incorrect.* For backups, not live access.

**C.** Windows EC2 with SMB  
❌ *Incorrect.* Not fully managed.

**D.** Amazon FSx for Windows File Server  
✅ *Correct.* Fully managed, supports SMB, ideal for media use cases.

**Question 250**

**Difficulty Level:** Medium  
**Category:** Security and Compliance

A company needs to store VPC Flow Logs for 90 days (frequent) and afterward (infrequent) access.

**What should a solutions architect do?**

**A.** Use CloudWatch with 90-day retention  
❌ *Incorrect.* Expensive for long-term storage.

**B.** Use Kinesis  
❌ *Incorrect.* Kinesis isn’t intended for log retention.

**C.** Use CloudTrail with S3 Intelligent-Tiering  
❌ *Incorrect.* CloudTrail is for API actions, not VPC logs.

**D.** Store in S3, move to S3 Standard-IA via Lifecycle policy  
✅ *Correct.* Cost-effective, flexible access after 90 days