

# AWS Certified Solutions Architect – Associate (SAA-C03)

## 100 Questions & Answers

Welcome to your complete AWS Certified Solutions Architect – Associate (SAA-C03) **practice questions collection**. This guide is designed not just to quiz you, but to build a deep understanding of AWS architectural decisions through **realistic, real-world scenarios** aligned with the actual exam blueprint.



## Learning Objectives and Expectations

You'll get:

- Realistic, scenario-based questions modeled after actual AWS exam structure
- Delivered in batches of 10 questions, followed by answers and explanations
- Reinforcement of core architectural principles: high availability, performance, security, and cost-efficiency
- Exposure to AWS service trade-offs and best practices under pressure
- 

## AWS Solutions Architect – Associate Domains

Each domain is weighted by importance in the exam. Domain 1 (Security) carries the most weight:

- **Domain 1: Design Secure Architectures – 30%**
- **Domain 2: Design Resilient Architectures – 26%**
- **Domain 3: Design High-Performing Architectures – 24%**
- **Domain 4: Design Cost-Optimized Architectures – 20%**

## Quick Reminder: How the Exam Works

- **Number of Questions:** 65
- **Format:** Multiple choice and multiple response, scenario-based
- **Time Limit:** 130 minutes
- **Passing Score:** 720/1000
- **Test Provider:** Pearson VUE (online proctored or testing center)

## Questions by Domain

| Domain          | Title                                | Questions Assigned | Question Numbers   |
|-----------------|--------------------------------------|--------------------|--|
| <b>Domain 1</b> | Design Secure Architectures          | 30 Questions       | Q2, Q4–5, Q12–13, Q20, Q26–27, Q35, Q40–42, Q44–45, Q51, Q53, Q55–57, Q60, Q66, Q69, Q71–72, Q75, Q83, Q95, Q97      |
| <b>Domain 2</b> | Design Resilient Architectures       | 26 Questions       | Q1, Q6–7, Q10, Q14, Q17–18, Q22, Q24, Q30, Q32, Q36, Q46, Q50, Q54, Q59, Q61, Q64, Q70, Q74, Q76, Q77, Q79, Q81, Q82 |
| <b>Domain 3</b> | Design High-Performing Architectures | 24 Questions       | Q3, Q8–9, Q11, Q15, Q21, Q23, Q25, Q28–29, Q31, Q34, Q37–38, Q47–48, Q52, Q58, Q63, Q73, Q80, Q84, Q87, Q98          |
| <b>Domain 4</b> | Design Cost-Optimized Architectures  | 20 Questions       | Q16, Q19, Q33, Q39, Q43, Q49, Q62, Q65, Q67–68, Q78, Q85–86, Q88–90, Q92–94, Q96, Q99–100                            |

## Remember — You Don't Need to Be Perfect to Pass!

The AWS SAA-C03 passing score is 720/1000, so you can miss about 13–17 scored questions and still pass. **Expect scenario-driven architecture decisions** — always focus on what the question is asking (security, cost, performance, or resilience) and **eliminate incorrect answers first**.

# Questions 1–10

## Q1.

A company is building a web application hosted on Amazon EC2 instances. The application must be highly available and automatically scale based on demand. Which architecture should the solutions architect recommend?

- A) Launch EC2 instances in a single Availability Zone with an Application Load Balancer
  - B) Use Auto Scaling groups across multiple Availability Zones behind an Application Load Balancer
  - C) Use EC2 Spot Instances with manual monitoring and scaling
  - D) Launch instances behind a Network Load Balancer in one Availability Zone
- 

## Q2.

A team stores sensitive financial reports in an Amazon S3 bucket. Compliance requirements mandate that all access to the bucket be logged and that objects be encrypted. What should the solutions architect do?

- A) Enable versioning and ACLs
  - B) Enable server-side encryption with SSE-S3 and enable S3 access logging
  - C) Use pre-signed URLs with SSE-C
  - D) Use RDS with transparent data encryption
- 

## Q3.

An application stores static content such as images and HTML pages in Amazon S3. To improve performance for global users, which solution should the architect implement?

- A) Enable versioning on the S3 bucket
  - B) Place the S3 bucket behind Amazon CloudFront
  - C) Enable Transfer Acceleration on the bucket
  - D) Use S3 Intelligent-Tiering
- 

## Q4.

A healthcare app must store patient data in AWS. Compliance requires that encryption keys never leave customer premises. What is the best encryption approach?

- A) SSE-S3
- B) SSE-KMS with default CMK
- C) SSE-KMS with custom key store
- D) Client-side encryption with customer-managed keys

---

**Q5.**

A startup wants to reduce its EC2 cost. All workloads are non-critical, stateless, and can tolerate interruptions. What should the architect recommend?

- A) Reserved Instances
  - B) Dedicated Hosts
  - C) Spot Instances
  - D) Savings Plans
- 

**Q6.**

An e-commerce site uses a MySQL RDS instance. During sales events, read queries spike and slow down the database. What should the solutions architect do?

- A) Increase instance size
  - B) Enable Multi-AZ
  - C) Use ElastiCache for caching
  - D) Use S3 for storage
- 

**Q7.**

A company runs web servers in two AZs. They want users to always reach the closest healthy server and automatically failover if one AZ fails. What should they use?

- A) Application Load Balancer
  - B) Network Load Balancer
  - C) Amazon Route 53 with failover routing
  - D) AWS Global Accelerator
- 

**Q8.**

A data analytics team needs to query logs stored in S3 using standard SQL without managing servers. What is the simplest solution?

- A) Redshift Spectrum
  - B) Athena
  - C) Glue
  - D) EMR with Hive
-

**Q9.**

A serverless application runs Lambda functions that access RDS. Under high load, connections fail. How can the architect resolve this?

- A) Use Aurora Serverless
  - B) Increase DB size
  - C) Use Amazon RDS Proxy
  - D) Use SQS between Lambda and RDS
- 

**Q10.**

A company's S3 bucket receives thousands of PUT and GET requests per second using sequential file names. Users report slow performance. What should the architect do?

- A) Enable object lock
  - B) Use random prefixes for object names
  - C) Enable versioning
  - D) Switch to EBS
- 

## Answers 1–10

**A1.**

Answer: B) Use Auto Scaling groups across multiple Availability Zones behind an Application Load Balancer

**Explanation:** This ensures high availability and automatic scaling across AZs.

---

**A2.**

Answer: B) Enable server-side encryption with SSE-S3 and enable S3 access logging

**Explanation:** SSE-S3 provides encryption at rest and access logs meet compliance requirements.

---

**A3.**

Answer: B) Place the S3 bucket behind Amazon CloudFront

**Explanation:** CloudFront caches content at edge locations to reduce latency.

---

**A4.**

Answer: D) Client-side encryption with customer-managed keys

**Explanation:** This approach ensures AWS never receives the keys, satisfying compliance.

---

**A5.**

Answer: C) Spot Instances

**Explanation:** Spot is best for fault-tolerant, cost-sensitive, and interruptible workloads.

---

**A6.**

Answer: C) Use ElastiCache for caching

**Explanation:** Caching offloads repeated read queries and improves DB performance.

---

**A7.**

Answer: C) Amazon Route 53 with failover routing

**Explanation:** Route 53 can route users to the closest healthy endpoint using health checks.

---

**A8.**

Answer: B) Athena

**Explanation:** Athena allows direct querying of S3 using SQL with no infrastructure.

---

**A9.**

Answer: C) Use Amazon RDS Proxy

**Explanation:** RDS Proxy manages connections and prevents exhaustion from bursty Lambda invocations.

---

**A10.**

Answer: B) Use random prefixes for object names

**Explanation:** S3 performance scales better when access patterns are distributed across prefixes.

# Questions 11–20

## Q11.

A company wants to isolate development and production environments while maintaining a shared billing account. Which AWS feature helps achieve this?

- A) AWS Organizations with separate accounts
  - B) IAM roles with policy separation
  - C) S3 bucket policies per environment
  - D) Security Groups and NACLs
- 

## Q12.

A serverless app uses Lambda to read/write from DynamoDB. Developers notice high latency on read-heavy workloads. What should the architect do?

- A) Enable DynamoDB Streams
  - B) Add Global Secondary Indexes
  - C) Use DynamoDB Accelerator (DAX)
  - D) Split the table into shards
- 

## Q13.

An app uses EC2 instances in a private subnet to retrieve data from S3. How can the architect ensure the lowest data transfer cost?

- A) Use NAT Gateway
  - B) Use Internet Gateway
  - C) Use Gateway VPC Endpoint
  - D) Use VPC peering
- 

## Q14.

A customer wants to archive infrequently accessed data in S3 with the lowest cost and is fine with long retrieval times. What should they choose?

- A) S3 Standard-IA
  - B) S3 One Zone-IA
  - C) S3 Glacier
  - D) S3 Glacier Deep Archive
-

**Q15.**

A real-time video processing application runs on a single EC2 instance. Users report frame drops and latency. How can performance be improved?

- A) Switch to a burstable T-series instance
  - B) Use EC2 Spot Instances
  - C) Use a compute-optimized EC2 instance
  - D) Migrate to Lambda
- 

**Q16.**

A team wants to run SQL queries on semi-structured data stored in S3, such as JSON and CSV files. What service should they use?

- A) Amazon Athena
  - B) Amazon Redshift
  - C) AWS Glue
  - D) Amazon RDS
- 

**Q17.**

An EC2 Auto Scaling group launches instances with a startup script that installs software. New instances take too long to become healthy. How can this be improved?

- A) Switch to Lambda
  - B) Pre-bake AMIs with required software
  - C) Use EC2 Spot Fleet
  - D) Increase instance type size
- 

**Q18.**

A company wants to centrally manage guardrails for multiple AWS accounts and restrict some services from being used. What feature should they use?

- A) IAM user policies
  - B) AWS Config
  - C) AWS Organizations with SCPs
  - D) VPC security groups
- 

**Q19.**

A static website hosted in S3 must use HTTPS and a custom domain name. What services should be used?



- A) Amazon CloudFront + ACM + Route 53
  - B) S3 Website Hosting + NAT Gateway
  - C) EC2 instance with Apache + SSL
  - D) Direct domain pointing to S3 with CNAME
- 

**Q20.**

A company needs low-latency, in-memory session storage for a web app running on EC2. What should the architect recommend?

- A) Amazon RDS
  - B) Amazon ElastiCache (Redis)
  - C) S3 Standard
  - D) DynamoDB
- 

## Answers 11–20

**A11.**

Answer: A) AWS Organizations with separate accounts

**Explanation:** This separates workloads while enabling consolidated billing.

---

**A12.**

Answer: C) Use DynamoDB Accelerator (DAX)

**Explanation:** DAX caches DynamoDB results for low-latency read performance.

---

**A13.**

Answer: C) Use Gateway VPC Endpoint

**Explanation:** This allows private, cost-free access to S3 from the VPC.

---

**A14.**

Answer: D) S3 Glacier Deep Archive

**Explanation:** Deep Archive offers the lowest-cost storage with long retrieval time.

---

**A15.**

Answer: C) Use a compute-optimized EC2 instance

**Explanation:** Compute-optimized instances are best for CPU-intensive workloads like video.

---

**A16.**

Answer: A) Amazon Athena

**Explanation:** Athena allows SQL queries on semi-structured S3 data with no infrastructure.

---

**A17.**

Answer: B) Pre-bake AMIs with required software

**Explanation:** Pre-baked AMIs significantly reduce launch and readiness time.

---

**A18.**

Answer: C) AWS Organizations with SCPs

**Explanation:** SCPs allow org-wide control over AWS service usage.

---

**A19.**

Answer: A) Amazon CloudFront + ACM + Route 53

**Explanation:** CloudFront enables HTTPS with ACM, and Route 53 allows domain mapping.

---

**A20.**

Answer: B) Amazon ElastiCache (Redis)

**Explanation:** Redis provides ultra-fast in-memory caching ideal for session data.

## Questions 21–30

### Q21.

A company is deploying a RESTful API using AWS services. They want to minimize management overhead and automatically scale with demand. Which combination of services should they use?

- A) EC2 + Nginx + RDS
  - B) API Gateway + Lambda + DynamoDB
  - C) Elastic Beanstalk + EC2 + MySQL
  - D) EC2 Auto Scaling + API Gateway + RDS
- 

### Q22.

A startup wants to run development environments in the cheapest way possible. The developers need access only from 9 AM to 5 PM, Monday to Friday. What should the solutions architect recommend?

- A) Buy Reserved Instances
  - B) Use Savings Plans
  - C) Use On-Demand and schedule stop/start with AWS Instance Scheduler
  - D) Use Dedicated Hosts
- 

### Q23.

A company's security team requires visibility into API activity across all AWS accounts in their organization. Which service provides this capability?

- A) Amazon Macie
  - B) AWS Config
  - C) AWS CloudTrail with Organization Trail
  - D) AWS Trusted Advisor
- 

### Q24.

A web application must allow users from multiple countries to experience the lowest latency possible. The app is deployed in a single region. What is the MOST effective way to reduce latency?

- A) Enable S3 Transfer Acceleration
- B) Deploy EC2 globally
- C) Use Amazon CloudFront
- D) Use Route 53 latency-based routing

---

**Q25.**

A Lambda function is failing due to TooManyRequestsException errors when accessing DynamoDB. What should be done?

- A) Increase provisioned throughput
  - B) Use DynamoDB Auto Scaling
  - C) Add retry logic with exponential backoff
  - D) Use RDS instead of DynamoDB
- 

**Q26.**

A financial services company must encrypt data stored in S3 using customer-managed keys. They want to control access to each object individually. What should they use?

- A) SSE-S3
  - B) SSE-KMS with CMKs
  - C) SSE-C
  - D) Client-side encryption
- 

**Q27.**

A company needs to share large files with external clients. Files should be accessible for a limited time only and must not be publicly listed. What is the BEST solution?

- A) Use S3 bucket with public read permissions
  - B) Use signed URLs for S3 objects
  - C) Email files as encrypted ZIP archives
  - D) Use S3 static website hosting
- 

**Q28.**

A developer is setting up CI/CD pipelines in AWS. They want to build, test, and deploy code automatically when changes are pushed to GitHub. Which AWS service should be used?

- A) CodeBuild
  - B) CodePipeline
  - C) CodeDeploy
  - D) CodeCommit
-

**Q29.**

An application sends 1000 messages per second between microservices. Messages must be processed in order. What service should be used?

- A) SQS Standard
  - B) SQS FIFO
  - C) SNS
  - D) Kinesis Firehose
- 

**Q30.**

A company has a fleet of EC2 instances and wants to automate the collection of inventory data (software versions, OS, patches). What is the best service to use?

- A) AWS Config
  - B) Amazon CloudWatch
  - C) AWS Systems Manager Inventory
  - D) AWS CloudTrail
- 

## Answers 21–30

**A21.**

Answer: B) API Gateway + Lambda + DynamoDB

**Explanation:** This is a fully serverless stack that automatically scales and minimizes management.

---

**A22.**

Answer: C) Use On-Demand and schedule stop/start with AWS Instance Scheduler

**Explanation:** Scheduling stop/start saves cost when instances aren't used.

---

**A23.**

Answer: C) AWS CloudTrail with Organization Trail

**Explanation:** Organization Trails record API events across all accounts centrally.

---

**A24.**

Answer: C) Use Amazon CloudFront

**Explanation:** CloudFront caches content closer to users, reducing latency globally.

---

**A25.**

Answer: C) Add retry logic with exponential backoff

**Explanation:** This is the best practice for throttling errors in DynamoDB from Lambda.

---

**A26.**

Answer: B) SSE-KMS with CMKs

**Explanation:** This allows fine-grained control over access and auditability.

---

**A27.**

Answer: B) Use signed URLs for S3 objects

**Explanation:** Signed URLs allow time-limited, secure access to individual objects.

---

**A28.**

Answer: B) CodePipeline

**Explanation:** CodePipeline integrates with GitHub to automate build, test, and deploy steps.

---

**A29.**

Answer: B) SQS FIFO

**Explanation:** FIFO queues guarantee exactly-once delivery and preserve order.

---

**A30.**

Answer: C) AWS Systems Manager Inventory

**Explanation:** This service automatically collects instance metadata and software inventory.

## Questions 31–40

### Q31.

A company wants to use AWS services to send email confirmations to users after they submit a form. They prefer a fully managed solution with high deliverability. Which service should they use?

- A) Amazon SNS
  - B) Amazon SES
  - C) Amazon SQS
  - D) Amazon Connect
- 

### Q32.

An e-commerce company wants to ensure that their product page loads as quickly as possible for international customers. The backend is hosted on EC2 in us-east-1. How can they minimize content load time?

- A) Enable S3 Transfer Acceleration
  - B) Deploy EC2 instances globally
  - C) Use Amazon CloudFront with edge caching
  - D) Add Elastic Load Balancer in multiple regions
- 

### Q33.

A user accidentally terminated a production EC2 instance. What feature can the architect enable to prevent this in the future?

- A) Termination protection
  - B) Auto Scaling
  - C) CloudTrail logging
  - D) EC2 encryption
- 

### Q34.

A company needs to design a solution that archives data for 7 years and requires minimal cost. The data is rarely accessed. Which solution should the architect choose?

- A) Store data in EBS Snapshots
- B) Store data in Amazon S3 Standard
- C) Store data in Amazon S3 Glacier Deep Archive
- D) Store data in DynamoDB with TTL enabled

---

**Q35.**

Which of the following allows you to enforce that no EC2 instances are launched without specific tags?

- A) IAM role trust policy
- B) S3 bucket policy
- C) AWS Config Rule
- D) Security Group rule

---

**Q36.**

Which AWS service enables automatic patching of Amazon EC2 instances?

- A) AWS Inspector
- B) AWS Systems Manager Patch Manager
- C) AWS Config
- D) CloudWatch Agent

---

**Q37.**

A company has a monolithic application and wants to migrate to a microservices architecture using containers. What service is most appropriate?

- A) Amazon SQS
- B) Amazon ECS
- C) Amazon Lambda
- D) Amazon Athena

---

**Q38.**

Which AWS service should be used to view historical configuration changes to AWS resources?

- A) Amazon CloudTrail
- B) AWS Config
- C) Amazon CloudWatch
- D) Trusted Advisor

---

**Q39.**

A media company is ingesting real-time video streams and needs to process them immediately. Which service should be used for stream ingestion?



- A) Amazon SNS
  - B) Amazon Kinesis Data Streams
  - C) Amazon SQS
  - D) AWS Step Functions
- 

**Q40.**

A company wants to ensure that root account usage is monitored and alerts are sent. What should be implemented?

- A) IAM access analyzer
  - B) CloudTrail with SNS notifications on root events
  - C) Trusted Advisor
  - D) GuardDuty
- 

## Answers 31–40

**A31.**

Answer: B) Amazon SES

**Explanation:** Amazon Simple Email Service is designed for sending transactional and marketing emails.

---

**A32.**

Answer: C) Use Amazon CloudFront with edge caching

**Explanation:** CloudFront caches static content close to users, improving load time globally.

---

**A33.**

Answer: A) Termination protection

**Explanation:** Termination protection prevents accidental instance deletion.

---

**A34.**

Answer: C) Store data in Amazon S3 Glacier Deep Archive

**Explanation:** Glacier Deep Archive is the lowest-cost long-term storage tier.

---

**A35.**

Answer: C) AWS Config Rule

**Explanation:** AWS Config can enforce compliance such as requiring specific resource tags.

---

**A36.**

Answer: B) AWS Systems Manager Patch Manager

**Explanation:** Patch Manager automates OS and software patching on EC2 instances.

---

**A37.**

Answer: B) Amazon ECS

**Explanation:** ECS is a container orchestration service ideal for running microservices.

---

**A38.**

Answer: B) AWS Config

**Explanation:** AWS Config tracks historical changes to AWS resource configurations.

---

**A39.**

Answer: B) Amazon Kinesis Data Streams

**Explanation:** Kinesis is used for high-throughput real-time stream processing.

---

**A40.**

Answer: B) CloudTrail with SNS notifications on root events

**Explanation:** CloudTrail tracks all API activity; SNS can notify on root usage.

## Questions 41–50

### Q41.

A startup wants to build a stateless backend service that can horizontally scale without managing infrastructure. Which AWS service should they use?

- A) Amazon EC2
  - B) AWS Lambda
  - C) Amazon RDS
  - D) Amazon Lightsail
- 

### Q42.

An enterprise customer wants to restrict access to an S3 bucket to only EC2 instances in a specific VPC. Which feature should the architect use?

- A) Bucket ACL
  - B) IAM User Policy
  - C) Bucket Policy with VPC endpoint condition
  - D) Enable versioning
- 

### Q43.

A user reports that their EC2 instance cannot access the internet. The instance is in a public subnet. What is the MOST likely reason?

- A) The instance lacks a public IP address
  - B) No NACL is attached
  - C) IAM role is missing
  - D) Route table has an entry to an S3 endpoint
- 

### Q44.

A mobile app authenticates users using Amazon Cognito. What benefit does Cognito provide in this architecture?

- A) Full database access
  - B) Temporary AWS credentials for access to AWS services
  - C) Static API keys for user accounts
  - D) Direct IAM role mapping per user
-

**Q45.**

Which of the following can reduce the risk of brute-force attacks on an EC2-based login form?

- A) Amazon Macie
  - B) WAF rate-based rules
  - C) GuardDuty alerts
  - D) S3 bucket encryption
- 

**Q46.**

A company needs a shared file system that can be mounted by thousands of EC2 instances across multiple AZs. What should they use?

- A) Amazon EBS
  - B) Amazon EFS
  - C) Amazon FSx for Windows
  - D) Amazon S3
- 

**Q47.**

An EC2 Auto Scaling group has unpredictable load during the day. Which scaling policy is most suitable?

- A) Scheduled scaling
  - B) Manual scaling
  - C) Dynamic scaling based on target tracking
  - D) Fixed-size scaling
- 

**Q48.**

A business collects clickstream data from millions of users and needs near real-time analytics. Which AWS service combination should they use?

- A) S3 + Athena
  - B) Kinesis Data Streams + Lambda
  - C) Redshift + EMR
  - D) RDS + EC2
- 

**Q49.**

An architect must design a system that automatically deletes old data from a DynamoDB table after 90 days. What should they use?

- A) AWS Glue
  - B) TTL (Time To Live) attribute
  - C) Lambda function scheduled with CloudWatch
  - D) DynamoDB Streams
- 

**Q50.**

A company wants to simplify management of secrets (API keys, DB passwords) across Lambda functions and EC2. What service should be used?

- A) AWS Secrets Manager
  - B) S3 with encryption
  - C) IAM roles
  - D) CloudHSM
- 

## Answers 41–50

**A41.**

Answer: B) AWS Lambda

**Explanation:** Lambda supports stateless, scalable, serverless compute.

---

**A42.**

Answer: C) Bucket Policy with VPC endpoint condition

**Explanation:** You can restrict S3 access by VPC using bucket policy conditions.

---

**A43.**

Answer: A) The instance lacks a public IP address

**Explanation:** Public subnets require public IPs and IGW to access the internet.

---

**A44.**

Answer: B) Temporary AWS credentials for access to AWS services

**Explanation:** Cognito federates identity and issues temporary credentials.

---

**A45.**

Answer: B) WAF rate-based rules

**Explanation:** Rate-based rules in WAF help block brute-force login attempts.

---

**A46.**

Answer: B) Amazon EFS

**Explanation:** EFS is a multi-AZ, scalable, shared file system for EC2.

---

**A47.**

Answer: C) Dynamic scaling based on target tracking

**Explanation:** Target tracking adjusts capacity to maintain a metric threshold.

---

**A48.**

Answer: B) Kinesis Data Streams + Lambda

**Explanation:** Kinesis captures data streams; Lambda processes them in near real-time.

---

**A49.**

Answer: B) TTL (Time To Live) attribute

**Explanation:** TTL in DynamoDB automatically deletes expired items.

---

**A50.**

Answer: A) AWS Secrets Manager

**Explanation:** Secrets Manager securely stores and rotates secrets automatically.

# Questions 51–60

## Q51.

A media company needs to store large volumes of frequently accessed video content with low latency. Which S3 storage class is most appropriate?

- A) S3 Standard
  - B) S3 Intelligent-Tiering
  - C) S3 Glacier
  - D) S3 One Zone-IA
- 

## Q52.

A company is using multiple EC2 instances behind an ALB. Some users report session timeouts while navigating. What is the best solution to maintain session state?

- A) Enable sticky sessions on the ALB
  - B) Use larger EC2 instance types
  - C) Increase the ALB timeout
  - D) Set up a Network Load Balancer
- 

## Q53.

A developer accidentally uploaded a private SSH key to a public S3 bucket. What should be done FIRST?

- A) Enable versioning on the bucket
  - B) Delete the object immediately
  - C) Rotate the associated credentials
  - D) Block public access at the account level
- 

## Q54.

An EC2 instance needs access to an S3 bucket. What is the most secure and scalable way to provide this access?

- A) Hardcode credentials in the app
  - B) Use an IAM user with access keys
  - C) Attach an IAM role to the EC2 instance
  - D) Generate a signed URL in advance
-

**Q55.**

A financial firm uses AWS to process sensitive data. It wants to ensure all EBS volumes are encrypted. How should this be enforced?

- A) Manually enable encryption when launching volumes
  - B) Use AWS Config rules to detect unencrypted volumes
  - C) Create an IAM policy to restrict EBS use
  - D) Tag encrypted volumes
- 

**Q56.**

An organization is seeing a spike in AWS costs. They want to identify idle resources. What service provides recommendations?

- A) CloudWatch
  - B) Trusted Advisor
  - C) CloudTrail
  - D) GuardDuty
- 

**Q57.**

Which feature ensures that traffic between EC2 instances in the same VPC does not leave AWS's private network?

- A) VPC Peering
  - B) Internet Gateway
  - C) Private IP addressing
  - D) Route 53
- 

**Q58.**

A company hosts a multi-tier app with web, app, and DB layers. Which security design principle should be followed?

- A) Single security group for all tiers
  - B) Shared IAM roles across tiers
  - C) Separate subnets and security groups per layer
  - D) Use NACLs only
- 

**Q59.**

Which AWS feature provides DDoS protection by default to all customers at no cost?



- A) AWS WAF
  - B) AWS Shield Standard
  - C) GuardDuty
  - D) VPC Flow Logs
- 

**Q60.**

A company needs to allow read-only access to specific S3 objects to an external vendor without giving access to the entire bucket. What is the best solution?

- A) Use bucket policy with vendor IP
  - B) Create IAM user with S3 read permissions
  - C) Use pre-signed URLs for object access
  - D) Enable static website hosting
- 

## Answers 51–60

**A51.**

Answer: A) S3 Standard

**Explanation:** S3 Standard is designed for frequently accessed, low-latency content like videos.

---

**A52.**

Answer: A) Enable sticky sessions on the ALB

**Explanation:** Sticky sessions route users to the same instance, maintaining session state.

---

**A53.**

Answer: B) Delete the object immediately

**Explanation:** Immediate deletion minimizes exposure; then rotate keys as needed.

---

**A54.**

Answer: C) Attach an IAM role to the EC2 instance

**Explanation:** IAM roles provide temporary, automatically rotated credentials.

---

**A55.**

Answer: B) Use AWS Config rules to detect unencrypted volumes

**Explanation:** AWS Config can enforce compliance by identifying misconfigured resources.

---

**A56.**

Answer: B) Trusted Advisor

**Explanation:** Trusted Advisor offers cost optimization checks, including idle resources.

---

**A57.**

Answer: C) Private IP addressing

**Explanation:** Traffic within a VPC using private IPs stays on AWS's internal network.

---

**A58.**

Answer: C) Separate subnets and security groups per layer

**Explanation:** Isolating tiers improves security and follows the principle of least privilege.

---

**A59.**

Answer: B) AWS Shield Standard

**Explanation:** Shield Standard provides automatic DDoS protection at no cost.

---

**A60.**

Answer: C) Use pre-signed URLs for object access

**Explanation:** Pre-signed URLs give time-limited access to specific S3 objects securely.

## Questions 61–70

### Q61.

A company deploys a web application on EC2 instances in two Availability Zones behind an Application Load Balancer. They notice that when one AZ becomes unhealthy, users experience intermittent failures. What is the MOST likely cause?

- A) The Auto Scaling group is set to minimum capacity of 1
  - B) Health checks are not properly configured on the ALB
  - C) Route 53 latency-based routing is not enabled
  - D) Sticky sessions are disabled
- 

### Q62.

A SaaS provider needs to onboard new customers by provisioning isolated environments per tenant. The solution should simplify billing and allow centralized governance. What should they use?

- A) Launch multiple EC2 instances in one account
  - B) Use AWS Organizations and create a separate account per tenant
  - C) Use IAM groups per tenant
  - D) Host all tenants in a single VPC using subnet segmentation
- 

### Q63.

A new application must support secure authentication from users' corporate Active Directory credentials. It will be deployed using a serverless architecture. Which service provides this capability?

- A) Amazon Cognito
  - B) AWS SSO
  - C) IAM with trust policy
  - D) AWS Directory Service
- 

### Q64.

A developer is launching an EC2 instance that must download large files from Amazon S3 during startup. The instance is in a private subnet. What design will reduce latency and avoid NAT Gateway charges?

- A) Use an Internet Gateway
- B) Use a NAT Instance

- C) Use a Gateway VPC Endpoint for S3
  - D) Enable S3 Transfer Acceleration
- 

**Q65.**

A team needs to test a new version of their web application without affecting production users. What is the MOST cost-effective way to do this using ALB?

- A) Use a separate ALB
  - B) Set up weighted target groups with traffic shifting
  - C) Deploy to a different region
  - D) Use EC2 tags to distinguish traffic
- 

**Q66.**

A company wants to detect whether sensitive data such as PII is being stored in Amazon S3. Which service helps achieve this?

- A) AWS Macie
  - B) GuardDuty
  - C) CloudTrail
  - D) AWS Config
- 

**Q67.**

A company is building an analytics dashboard that needs to query petabytes of data stored in S3 using SQL. They want to avoid infrastructure management. What should they use?

- A) Amazon Redshift
  - B) Amazon Athena
  - C) Amazon EMR
  - D) Amazon RDS
- 

**Q68.**

A mobile app needs to upload user-generated content to S3 securely. The backend must NOT proxy the upload traffic. What solution should the architect implement?

- A) Use S3 pre-signed URLs
- B) Use S3 static website hosting
- C) Use Lambda as a proxy for uploads
- D) Use Amazon CloudFront to POST to S3

---

**Q69.**

A security team wants to ensure that only encrypted Amazon EBS volumes can be created. What is the BEST way to enforce this?

- A) Apply IAM policies
  - B) Use AWS Config rules
  - C) Enable default encryption in EC2 settings
  - D) Attach KMS key to volumes
- 

**Q70.**

A web app uses EC2 and RDS. The app performs slowly under unpredictable high user traffic. What is the BEST way to improve performance and reliability?

- A) Increase EC2 instance size
  - B) Add Multi-AZ to RDS
  - C) Implement Auto Scaling for EC2 and read replicas for RDS
  - D) Upgrade RDS to Aurora
- 

## Answers 61–70

**A61.**

Answer: B) Health checks are not properly configured on the ALB

**Explanation:** Improper health checks may prevent traffic from shifting away from unhealthy AZs.

---

**A62.**

Answer: B) Use AWS Organizations and create a separate account per tenant

**Explanation:** Provides isolation, centralized governance, and consolidated billing.

---

**A63.**

Answer: A) Amazon Cognito

**Explanation:** Cognito supports federated identity and integrates with SAML-based corporate credentials.

---

**A64.**

Answer: C) Use a Gateway VPC Endpoint for S3

**Explanation:** This provides direct access to S3 from private subnets without NAT costs.

---

**A65.**

Answer: B) Set up weighted target groups with traffic shifting

**Explanation:** Weighted target groups let you run blue/green or canary deployments behind an ALB.

---

**A66.**

Answer: A) AWS Macie

**Explanation:** Macie uses ML to detect sensitive data in S3 such as PII.

---

**A67.**

Answer: B) Amazon Athena

**Explanation:** Athena lets users query data in S3 using SQL without provisioning infrastructure.

---

**A68.**

Answer: A) Use S3 pre-signed URLs

**Explanation:** Pre-signed URLs allow secure direct uploads from clients without routing through the backend.

---

**A69.**

Answer: B) Use AWS Config rules

**Explanation:** Config rules can enforce compliance such as encryption requirements for EBS volumes.

---

**A70.**

Answer: C) Implement Auto Scaling for EC2 and read replicas for RDS

**Explanation:** Scaling the web and DB tiers horizontally improves performance under unpredictable load.

## Questions 71–80

### Q71.

A company uses AWS CloudTrail to log all account activity. The security team wants to be alerted if anyone disables logging. What should the architect do?

- A) Create a CloudWatch alarm for the StopLogging API call
  - B) Use AWS Macie to scan logs
  - C) Enable encryption for CloudTrail
  - D) Enable GuardDuty
- 

### Q72.

A developer wants to restrict access to an S3 bucket so only a specific IAM role can read objects. What should they do?

- A) Use a bucket ACL to allow role access
  - B) Modify the IAM role's inline policy
  - C) Attach a bucket policy with a condition for the role ARN
  - D) Use a signed URL
- 

### Q73.

A healthcare app must comply with HIPAA. What AWS feature helps securely store patient records in transit and at rest?

- A) Enable S3 event notifications
  - B) Use SSE-KMS for encryption and HTTPS for data transmission
  - C) Use versioning
  - D) Enable cross-region replication
- 

### Q74.

An EC2 Auto Scaling group has a scaling policy based on CPU usage. During peak traffic, new instances are launched but take too long to serve users. What can help?

- A) Use larger instance types
  - B) Use pre-baked AMIs with software installed
  - C) Switch to Lambda
  - D) Enable instance hibernation
-

**Q75.**

A customer stores monthly invoices in an S3 bucket. The company wants to ensure invoices cannot be accidentally deleted or modified for 7 years. What should they do?

- A) Enable versioning
  - B) Use Object Lock in compliance mode
  - C) Use S3 One Zone-IA
  - D) Enable lifecycle expiration
- 

**Q76.**

Which AWS service provides real-time analysis of VPC traffic to detect threats?

- A) CloudWatch Logs
  - B) GuardDuty
  - C) Config
  - D) CloudTrail
- 

**Q77.**

A startup uses AWS Lambda for an event-driven app. They want to monitor function performance, invocations, and errors. What should they use?

- A) CloudTrail
  - B) CloudWatch Logs and Metrics
  - C) AWS Config
  - D) X-Ray only
- 

**Q78.**

A SaaS provider wants to ensure that each customer's data is logically isolated but hosted in the same DynamoDB table. What feature supports this design?

- A) DynamoDB Global Tables
  - B) Partition key per tenant
  - C) TTL per item
  - D) Separate tables per customer
- 

**Q79.**

Which service should be used to automate the deployment of infrastructure using code?



- A) AWS CodeBuild
  - B) AWS CodeDeploy
  - C) AWS CloudFormation
  - D) AWS CodeCommit
- 

#### Q80.

A company is migrating a workload from on-premises to AWS. They need secure, encrypted, and consistent network performance. What is the BEST solution?

- A) Site-to-Site VPN
  - B) Internet Gateway
  - C) VPC Peering
  - D) AWS Direct Connect
- 

## Answers 71–80

#### A71.

Answer: A) Create a CloudWatch alarm for the StopLogging API call

**Explanation:** This enables real-time detection of attempts to disable CloudTrail logging.

---

#### A72.

Answer: C) Attach a bucket policy with a condition for the role ARN

**Explanation:** Bucket policies can restrict access to specific IAM roles using conditions.

---

#### A73.

Answer: B) Use SSE-KMS for encryption and HTTPS for data transmission

**Explanation:** Combines encryption at rest and in transit, satisfying HIPAA encryption requirements.

---

#### A74.

Answer: B) Use pre-baked AMIs with software installed

**Explanation:** Reduces launch time by avoiding time-consuming provisioning steps.

---

**A75.**

Answer: B) Use Object Lock in compliance mode

**Explanation:** Prevents deletion or modification of objects for a defined retention period.

---

**A76.**

Answer: B) GuardDuty

**Explanation:** Analyzes VPC flow logs and CloudTrail for threats and anomalies.

---

**A77.**

Answer: B) CloudWatch Logs and Metrics

**Explanation:** CloudWatch provides metrics like duration, errors, and invocation counts for Lambda.

---

**A78.**

Answer: B) Partition key per tenant

**Explanation:** Logical separation is achieved using a tenant identifier as the partition key.

---

**A79.**

Answer: C) AWS CloudFormation

**Explanation:** CloudFormation automates infrastructure provisioning using templates.

---

**A80.**

Answer: D) AWS Direct Connect

**Explanation:** Provides secure, consistent, high-bandwidth, and encrypted connectivity.

# Questions 81–90

## Q81.

A solutions architect needs to migrate an existing web application to AWS. The app consists of a web tier and a MySQL database. The architecture must support automatic failover with minimal operational overhead. What should the architect choose?

- A) EC2 + MySQL installed manually
  - B) Elastic Beanstalk + RDS Multi-AZ
  - C) EC2 Auto Scaling + MySQL on EBS
  - D) Lambda + Aurora Serverless
- 

## Q82.

A company uses Amazon RDS for PostgreSQL in a single AZ. They are concerned about data loss and availability. What change should they make?

- A) Increase instance type
  - B) Enable Multi-AZ deployment
  - C) Add more read replicas
  - D) Backup the DB manually every hour
- 

## Q83.

An application stores configuration data in AWS Systems Manager Parameter Store. Some parameters must be encrypted. What feature should the architect use?

- A) Store as plain text
  - B) Enable versioning
  - C) Use SecureString with KMS key
  - D) Use Lambda to encrypt the values
- 

## Q84.

A development team frequently provisions and tears down test environments. They want a cost-effective way to ensure their infrastructure is deployed consistently. What is the best solution?

- A) Use CloudFormation templates
- B) Use EC2 launch templates
- C) Manually provision via console
- D) Use snapshots for reuse

---

**Q85.**

A client needs to serve static web content with low latency to users in multiple continents. What architecture should be used?

- A) S3 + CloudFront
  - B) EC2 + NGINX
  - C) S3 One Zone-IA
  - D) Lambda + API Gateway
- 

**Q86.**

An internal tool is only used by employees on the corporate network. What is the most secure way to host this tool on AWS?

- A) Host on EC2 with public IP
  - B) Use S3 static hosting
  - C) Place it in a private subnet behind a VPN
  - D) Use Lambda with API Gateway
- 

**Q87.**

An application is deployed in multiple AZs using EC2 and an ALB. Users report that uploaded files are missing after switching availability zones. What is the best fix?

- A) Use S3 for shared file storage
  - B) Sync files manually between instances
  - C) Use EBS and snapshot replication
  - D) Increase ALB timeout
- 

**Q88.**

A company wants to manage SSL certificates and automatically renew them. Which service should be used?

- A) AWS Certificate Manager
  - B) CloudHSM
  - C) IAM Server Certificates
  - D) Route 53
-

**Q89.**

Which AWS service is best suited for real-time application monitoring, dashboarding, and alarms?

- A) AWS X-Ray
  - B) AWS CloudWatch
  - C) AWS Config
  - D) AWS Macie
- 

**Q90.**

Which VPC component is required to allow internet access to resources in a public subnet?

- A) Security Group
  - B) Network ACL
  - C) NAT Gateway
  - D) Internet Gateway
- 

## Answers 81–90

**A81.**

Answer: B) Elastic Beanstalk + RDS Multi-AZ

**Explanation:** Beanstalk simplifies deployment, and Multi-AZ ensures database failover.

---

**A82.**

Answer: B) Enable Multi-AZ deployment

**Explanation:** Multi-AZ improves availability and minimizes data loss.

---

**A83.**

Answer: C) Use SecureString with KMS key

**Explanation:** SecureString ensures encryption at rest using KMS.

---

**A84.**

Answer: A) Use CloudFormation templates

**Explanation:** CloudFormation ensures consistent, repeatable infrastructure as code.

---

**A85.**

Answer: A) S3 + CloudFront

**Explanation:** S3 stores static content; CloudFront delivers it globally with low latency.

---

**A86.**

Answer: C) Place it in a private subnet behind a VPN

**Explanation:** Hosting in a private subnet and requiring VPN ensures access only from internal users.

---

**A87.**

Answer: A) Use S3 for shared file storage

**Explanation:** S3 provides shared, persistent storage accessible from all AZs.

---

**A88.**

Answer: A) AWS Certificate Manager

**Explanation:** ACM handles SSL certificate provisioning and renewal automatically.

---

**A89.**

Answer: B) AWS CloudWatch

**Explanation:** CloudWatch provides monitoring, logs, dashboards, and alerting.

---

**A90.**

Answer: D) Internet Gateway

**Explanation:** An IGW is required for internet access from public subnets.

## Questions 91–100

### Q91.

A company wants to reduce costs on their development EC2 instances, which are only used during weekdays. What is the MOST effective solution?

- A) Switch to Spot Instances
  - B) Purchase Reserved Instances
  - C) Use Savings Plans
  - D) Schedule automatic stop/start during off-hours
- 

### Q92.

A security engineer needs to audit all configuration changes made to AWS resources, including who made the change and when. Which service provides this information?

- A) AWS Config
  - B) CloudWatch
  - C) IAM Access Analyzer
  - D) Macie
- 

### Q93.

An application running on EC2 reads from and writes to a DynamoDB table. The app is being throttled. What is the BEST solution?

- A) Increase EC2 instance size
  - B) Enable DynamoDB Auto Scaling
  - C) Convert to provisioned mode with low read/write capacity
  - D) Use Kinesis to batch the writes
- 

### Q94.

A customer is deploying a mobile app that allows users to upload profile pictures. How can the architect securely allow uploads directly to S3 without exposing credentials?

- A) IAM access keys in the app
  - B) Lambda function to upload objects
  - C) Use pre-signed URLs generated by backend
  - D) Attach IAM role to the app
-

**Q95.**

A government agency has strict compliance rules that require physical hardware separation for workloads. What Amazon EC2 option should be selected?

- A) On-Demand Instances
  - B) EC2 Dedicated Instances
  - C) EC2 Spot Instances
  - D) EC2 Dedicated Hosts
- 

**Q96.**

Which AWS service can run SQL queries against data stored in S3 and return results without provisioning infrastructure?

- A) Redshift
  - B) RDS
  - C) Athena
  - D) Glue
- 

**Q97.**

A company wants to enforce password complexity and rotation policies for IAM users. What should they use?

- A) IAM inline policies
  - B) IAM roles
  - C) AWS Organizations
  - D) IAM Account Password Policy
- 

**Q98.**

A developer needs to run a containerized application without managing servers or clusters. Which AWS service is the BEST choice?

- A) EC2 with Docker installed
  - B) ECS on EC2
  - C) Fargate
  - D) EKS
- 

**Q99.**

Which of the following automatically backs up Amazon RDS databases and allows point-in-time recovery?



- A) Manual snapshots
  - B) AWS Backup
  - C) RDS automated backups
  - D) EBS snapshots
- 

**Q100.**

A team is building an architecture that must withstand the loss of an entire Availability Zone. What is the best practice?

- A) Deploy in a single AZ with snapshots
  - B) Use EC2 Auto Scaling across multiple AZs
  - C) Use Reserved Instances in one AZ
  - D) Use a large EC2 instance in one region
- 

## Answers 91–100

**A91.**

Answer: D) Schedule automatic stop/start during off-hours

**Explanation:** This approach eliminates compute charges during idle periods and is ideal for dev workloads.

---

**A92.**

Answer: A) AWS Config

**Explanation:** Config provides a history of resource configurations and who made changes.

---

**A93.**

Answer: B) Enable DynamoDB Auto Scaling

**Explanation:** Auto Scaling adjusts read/write capacity to match application demand.

---

**A94.**

Answer: C) Use pre-signed URLs generated by backend

**Explanation:** Pre-signed URLs allow secure, temporary, authenticated access without exposing credentials.

---

**A95.**

Answer: D) EC2 Dedicated Hosts

**Explanation:** Dedicated Hosts provide physical separation per compliance needs.

---

**A96.**

Answer: C) Athena

**Explanation:** Athena enables SQL querying of S3 data with no server provisioning.

---

**A97.**

Answer: D) IAM Account Password Policy

**Explanation:** This policy enforces complexity, rotation, and reuse requirements for IAM users.

---

**A98.**

Answer: C) Fargate

**Explanation:** Fargate runs containers without managing EC2 infrastructure or clusters.

---

**A99.**

Answer: C) RDS automated backups

**Explanation:** Automated backups allow point-in-time recovery and are enabled by default.

---

**A100.**

Answer: B) Use EC2 Auto Scaling across multiple AZs

**Explanation:** Multi-AZ Auto Scaling ensures high availability and resilience against AZ failure.