CERT-PASS.com

Pass Your Cloud Cert. First Try.

Stop guessing. Start passing. Premium practice exams with real-world scenarios.

DATABRICKS | AWS | AZURE | GCP | SNOWFLAKE

- ✔ 93% First-Try Pass Rate
- ✔ Extensive Question Bank
- ✔ Updated for Latest Exams

THE ADVANTAGE

Exam-Accurate Content

Authored by certified engineers. Every question mirrors the real exam's structure, wording, and difficulty. No braindumps.

Deep Explanations

Don't just memorize. Every answer explains exactly "why A" is correct and "why not B, C, D" to build true comprehension.

Topic Analytics & Focus

Pinpoint your weak spots instantly with official blueprint-weighted scoring. Block distractions with Focus Mode.

Comprehensive Guides

Every single exam includes a fully structured curriculum. Learn the core concepts before diving into the practice tests.

THE PROCESS

01 **Pick Your Target Exam**

Browse our official catalog, select your certification, and generate your custom study plan.

02 **Practice & Analyze Data**

Take weighted practice exams. Get immediate feedback and watch readiness update in real time.

03 **Pass With Confidence**

Walk into the testing center backed by data, not hope. Join the 93% who pass on the first attempt.

Ready to get certified?

Start free today — no credit card required.

CERT-PASS

AWS AWS Solutions Architect – Associate (SAA-C03)

Free Practice Questions Preview

Here are 15 sample questions to help you get started. Unlock the full exam to access all 65+ questions with detailed explanations.

Question 1 : Domain 1 - Design Secure Architectures

A company wants to limit an S3 bucket to only accounts within its AWS Organisation with least operational overhead. Which solution meets these requirements?

A. aws:PrincipalOrgID condition in bucket policy

B. aws:PrincipalOrgPaths per OU

C. CloudTrail events + manual policy updates

D. Tag users + aws:PrincipalTag

Answer: A
aws:PrincipalOrgID covers all current and future org accounts in a single condition—no ongoing updates needed. Other options require more complex or manual maintenance.

Question 2 : Domain 1 - Design Secure Architectures

An EC2 instance in a VPC needs to access an S3 bucket without internet connectivity. Which solution meets this requirement?

A. Gateway VPC endpoint to S3

B. Stream to CloudWatch Logs then export

C. Instance profile (IAM role) on EC2

D. API Gateway + PrivateLink

Answer: A
A gateway VPC endpoint routes S3 traffic within the AWS network, requiring no internet gateway or NAT. An instance profile grants permissions but not private network connectivity.

Question 3 : Domain 1 - Design Secure Architectures

EC2 instances connect to Aurora using credentials in a local file. Which solution minimises credential management overhead?

A. AWS Secrets Manager + automatic rotation

B. Systems Manager Parameter Store + rotation

C. Encrypted S3 bucket for credentials

D. Encrypted EBS volume per instance

Answer: A
Secrets Manager is purpose-built for managing secrets with native automatic rotation, IAM integration, and audit via CloudTrail. Parameter Store lacks native rotation; S3 and EBS require custom logic.

Question 4 : Domain 1 - Design Secure Architectures

Rotate RDS for MySQL credentials across multiple AWS Regions monthly with least operational overhead. Which solution meets these requirements?

A. Secrets Manager + multi-Region replication + scheduled rotation

B. Parameter Store + multi-Region replication

C. S3 (SSE) + EventBridge + Lambda

D. KMS multi-Region keys + DynamoDB global table + Lambda

Answer: A
Secrets Manager natively supports multi-Region secret replication and scheduled automatic rotation—no custom code needed. All other options require significant custom development.

Question 5 : Domain 1 - Design Secure Architectures

Company migrated to AWS and needs to replicate on-premises traffic flow inspection and filtering for its production VP C. Which service meets this requirement?

A. Amazon GuardDuty

B. Traffic Mirroring

C. AWS Network Firewall

D. AWS Firewall Manager

Answer: C
AWS Network Firewall provides inline deep packet inspection and traffic filtering at Layers 3, 4, and 7—directly matching on-premises inspection server behaviour. GuardDuty detects threats but does not filter traffic.

Question 6 : Domain 1 - Design Secure Architectures

Data lake on S3 + RDS PostgreSQL. Management needs full access; other employees need limited access to visualisations. Which solution meets these requirements?

A. QuickSight dashboards shared via IAM roles

B. QuickSight dashboards shared via users and groups

C. Glue + ETL ? S3 reports with bucket policies

D. Glue + Athena Federated Query ? S3 reports

Answer: B
QuickSight connects to both S3 and RDS and supports native user/group sharing for granular dashboard access control. IAM roles control resource access, not QuickSight dashboard access; Glue/Athena produce static reports.

Question 7 : Domain 1 - Design Secure Architectures

Two EC2 instances need access to an S3 bucket for document storage. Which solution is most appropriate?

A. IAM role with S3 access attached to EC2 instances

B. IAM policy attached directly to EC2

C. IAM group attached to EC2

D. IAM user credentials stored on EC2

Answer: A
IAM roles provide temporary, automatically-rotated credentials to EC2 instances. Policies cannot be attached directly to EC2; groups are for users only; storing IAM user credentials on EC2 is a security anti-pattern.

Question 8 : Domain 1 - Design Secure Architectures

Three-tier web app with third-party firewall appliance in inspection VP C. All inbound traffic must be inspected before reaching web servers with least operational overhead. Which solution meets these requirements?

A. NLB in public subnet routes to appliance

B. ALB in public subnet routes to appliance

C. Transit gateway in inspection VPC

D. Gateway Load Balancer + GWLB endpoint in inspection VPC

Answer: D
GWLB is purpose-built for inline traffic inspection via virtual appliances. A GWLB endpoint transparently intercepts and forwards traffic to the appliance—fully managed and auto-scaling. NLB/ALB are not designed for transparent packet redirection; Transit Gateway requires complex routing.

Question 9 : Domain 1 - Design Secure Architectures

IAM user accidentally exposed AWS credentials on a public code repository. What immediate steps should be taken? (Choose TWO)

A. Remove the IAM user's permissions

B. Delete the exposed access key

C. Rotate the exposed access key

D. Enable MFA for the IAM user

E. Invalidate temporary credentials by contacting AWS Support

Answer: BC
Immediately deactivate/delete the exposed key (B) to prevent unauthorised use and rotate/create a new key (C) to restore legitimate access. Removing permissions (A) would break operations; MFA (D) doesn't revoke already-exposed keys; temporary credentials expire on their own (E).

Question 10 : Domain 1 - Design Secure Architectures

Company needs to ensure data at rest in S3 is encrypted using keys they fully control. Which solution meets this requirement?

A. S3 managed keys (SSE-S3)

B. AWS KMS managed keys (SSE-KMS)

C. Customer-provided keys (SSE-C)

D. Client-side encryption

Answer: B
SSE-KMS uses AWS KMS CMKs that the company creates, controls, and can audit via CloudTrail—full key control with managed infrastructure. SSE-S3 is AWS-managed; SSE-C requires managing keys outside AWS; client-side encryption adds application complexity.

Question 11 : Domain 1 - Design Secure Architectures

Solutions architect needs to ensure VPC traffic to and from on-premises uses dedicated bandwidth with consistent latency. Which solution meets this requirement?

A. Site-to-Site VPN

B. AWS Direct Connect

C. AWS Transit Gateway

D. VPC Peering

Answer: B
AWS Direct Connect provides a dedicated private network connection with consistent latency and predictable bandwidth—not shared with public internet traffic. VPN traverses the public internet with variable performance; Transit Gateway and VPC Peering connect AWS-to-AWS networks.

Question 12 : Domain 1 - Design Secure Architectures

Company uses a bastion host in a public subnet to SSH into application instances in private subnets. On-premises engineers need access. Which TWO security group rules should be configured? (Choose TWO)

A. Allow inbound access from application instances to bastion

B. Allow inbound access from internal IP range to bastion

C. Allow inbound access from company's external IP range to bastion

D. Allow inbound SSH from bastion private IP to application instances

E. Allow inbound SSH from bastion public IP to application instances

Answer: CD
C: The bastion must allow inbound SSH from the company's external IP range (traffic from on-premises arrives via public internet). D: Application instances should allow SSH only from the bastion's private IP—keeping them unreachable from the internet. Option B (internal IP) won't work because on-premises traffic arrives with the external IP.

Question 13 : Domain 1 - Design Secure Architectures

Company needs to detect and remediate security vulnerabilities in EC2 instances automatically. Which service meets this requirement?

A. AWS Config

B. Amazon Inspector

C. AWS Trusted Advisor

D. Amazon GuardDuty

Answer: B
Amazon Inspector automatically assesses EC2 instances and container images for software vulnerabilities and unintended network exposure, generating findings with severity scores. AWS Config tracks configuration compliance; Trusted Advisor gives best-practice checks; GuardDuty detects threats in logs/network traffic but doesn't scan for CVEs.

Question 14 : Domain 1 - Design Secure Architectures

Two-tier web app: public-facing web tier on EC2 in public subnet; SQL Server on EC2 in private subnet. Which TWO security group rules should be configured? (Choose TWO)

A. Web tier SG: allow inbound port 443 from 0.0.0.0/0

B. Web tier SG: allow outbound port 443 from 0.0.0.0/0

C. DB tier SG: allow inbound port 1433 from web tier SG

D. DB tier SG: allow outbound ports 443 and 1433 to web tier SG

E. DB tier SG: allow inbound ports 443 and 1433 from web tier SG

Answer: AC
A: The web tier must accept HTTPS from the internet (0.0.0.0/0 on 443). C: The database tier must accept SQL Server connections (port 1433) only from the web tier's security group—not from the internet. Outbound rules are not needed because SGs are stateful; port 443 is not needed on the DB tier.

Question 15 : Domain 1 - Design Secure Architectures

A developer accidentally deleted a DynamoDB table with production data. How can this be prevented in future?

A. Enable DynamoDB point-in-time recovery (PITR)

B. Apply an IAM policy that denies DeleteTable for developers

C. Enable DynamoDB Streams

D. Use AWS Backup to schedule daily backups

Answer: B

An IAM deny policy on DeleteTable at the developer role level prevents the action entirely—addressing the root cause. PITR (A) and backups (D) enable recovery but don't prevent deletion; Streams (C) is for change data capture, not access control.