CERT-PASS

AWS AWS Solutions Architect – Associate (SAA-C03)

Free Practice Questions Preview

Here are 35 sample questions to help you get started. Unlock the full exam to access all 1008+ questions with detailed explanations.

Question 1 : Design Secure Architectures

A media startup runs a payments API in private subnets. The application must read objects from Amazon S3 without using the internet, NAT gateways, or public IP addresses. Which design should the solutions architect recommend? In this data platform migration, the environment includes 60 branch offices; assume all services are available in the selected Region. The documented scale target is 1,013 users or events for this scenario.

A. Attach an internet gateway to the private subnets and allow outbound HTTPS.

B. Create a NAT gateway in each Availability Zone and route S3 traffic through the NAT gateways.

C. Deploy an Application Load Balancer in front of Amazon S3 and restrict it with security groups.

D. Create a gateway VPC endpoint for Amazon S3 and associate it with the private subnet route tables.

Answer: D
An S3 gateway endpoint provides private S3 access from a VPC and avoids NAT gateway processing charges. The tempting wrong choice adds complexity without meeting the key requirement: NAT gateways can reach S3, but they do not satisfy the private-no-NAT requirement and add cost.

Question 2 : Design Secure Architectures

A public sector agency uses multiple AWS accounts for a data lake ingestion workflow. Security wants to prevent account administrators from disabling AWS CloudTrail or leaving AWS Organizations. What is the most effective control? The current pattern has steady weekday traffic and the team wants an AWS managed option. In this regional expansion, the environment includes 80 million requests/month; assume all services are available in the selected Region. The documented scale target is 1,026 users or events for this scenario.

A. Configure security groups to deny access to AWS Organizations endpoints.

B. Use AWS WAF rules to block CloudTrail API calls.

C. Apply service control policies in AWS Organizations that deny the prohibited actions for the target OUs.

D. Create IAM policies in each account that deny the actions to all roles except administrators.

Answer: C
SCPs are organization-level guardrails that restrict actions even when principals have local administrator permissions. This is a common trap because it solves only part of the requirement: IAM policies inside each account are weaker because privileged local administrators can change them unless constrained by an SCP.

Question 3 : Design Secure Architectures

A partner company must upload reports to one prefix in an S3 bucket owned by a education platform. The company must not create long-term IAM users for the partner. Which approach best follows least privilege? The architects prefer a design with minimal custom operations and clear exam-style tradeoffs. In this security review, the environment includes 40 production VPCs; assume all services are available in the selected Region. The documented scale target is 1,039 users or events for this scenario.

A. Create an IAM user in the bucket account and email the access keys to the partner.

B. Make the S3 bucket public and rely on unpredictable object names.

C. Use a cross-account IAM role or bucket policy that grants the partner account permission only to the required prefix.

D. Use a security group rule that permits the partner IP range to access the bucket.

Answer: C
Cross-account access with a resource policy or role avoids long-term shared credentials and can be scoped to a specific prefix. This is a common trap because it solves only part of the requirement: S3 buckets are not protected by security groups, and IP-based access alone is not a full identity and least-privilege design.

Question 4 : Design Secure Architectures

A mobile app for a retail company needs user sign-up, sign-in, and temporary AWS credentials for authenticated users to access restricted resources. Which service combination should be used? The solution must be suitable for production and avoid unnecessary operational risk. In this performance tuning sprint, the environment includes 300 GB/day; assume all services are available in the selected Region. The documented scale target is 1,052 users or events for this scenario.

A. AWS Organizations accounts for every mobile user.

B. AWS Directory Service Simple AD exposed to the internet.

C. Amazon Cognito user pools and identity pools.

D. AWS IAM users for every mobile user.

Answer: C
Cognito handles application identity and can exchange authenticated identities for temporary AWS credentials. The tempting wrong choice adds complexity without meeting the key requirement: IAM users for app consumers create long-term credentials and do not scale securely for mobile sign-in.

Question 5 : Design Secure Architectures

A media startup stores regulated records in S3. Records must be retained for seven years and must not be deleted by any user, including administrators, during retention. What should be configured? The team needs the BEST answer, not merely a solution that can work. In this cost review cycle, the environment includes 18 Availability Zones; assume all services are available in the selected Region. The documented scale target is 1,065 users or events for this scenario.

A. S3 Intelligent-Tiering with lifecycle expiration disabled.

B. A bucket policy that denies s3:DeleteObject to all IAM users.

C. S3 Object Lock in compliance mode with an appropriate retention period.

D. S3 server access logging with MFA Delete disabled.

Answer: C
S3 Object Lock compliance mode provides WORM retention that administrators cannot bypass during the retention period. The best wrong answer is close, but it misses the stated constraint: A deny-delete bucket policy can often be changed by sufficiently privileged administrators, so it does not provide the same immutable retention.

Question 6 : Design Secure Architectures

An EC2 instance in a private subnet must retrieve database credentials securely. The team wants automatic rotation and no secrets stored in user data or environment variables. What is the best solution? In this resilience test, the environment includes 12 microservices; assume all services are available in the selected Region. The documented scale target is 1,078 users or events for this scenario.

A. Put the password in Systems Manager Parameter Store as a plain String parameter.

B. Store the password in an encrypted AMI and rotate the AMI monthly.

C. Embed the password in EC2 user data and restrict access with a security group.

D. Store the credential in AWS Secrets Manager, enable rotation, and allow the instance role to retrieve the secret.

Answer: D
Secrets Manager supports managed secret retrieval and rotation through IAM-controlled access. The best wrong answer is close, but it misses the stated constraint: Parameter Store can store secure strings, but a plain String does not protect the secret and does not satisfy the secure-rotation requirement.

Question 7 : Design Secure Architectures

A mobile backend uses an Application Load Balancer. The security team requires TLS termination with managed certificates and automatic certificate renewal. What should the architect configure? The current pattern has unpredictable daily spikes and the team wants an AWS managed option. In this audit preparation, the environment includes 25 TB; assume all services are available in the selected Region. The documented scale target is 1,091 users or events for this scenario.

A. Upload self-signed certificates to each EC2 instance and renew them manually.

B. Use a Network ACL to encrypt traffic between clients and the load balancer.

C. Use AWS Certificate Manager certificates on the HTTPS listener of the Application Load Balancer.

D. Use AWS KMS keys directly as TLS certificates on the listener.

Answer: C
ACM integrates with ALB listeners and can renew eligible public certificates automatically. The best wrong answer is close, but it misses the stated constraint: Self-signed certificates on instances add manual operations and do not provide managed public TLS termination at the ALB.

Question 8 : Design Secure Architectures

A company needs centralized threat detection across all accounts and Regions for workloads including S3, EC2, and IAM activity. Which AWS service should be enabled with delegated administration? The architects prefer a design with minimal custom operations and clear exam-style tradeoffs. In this mobile rollout, the environment includes 200 developer accounts;

assume all services are available in the selected Region. The documented scale target is 1,104 users or events for this scenario.

A. Amazon Inspector only for S3 bucket policies.

B. AWS Trusted Advisor only.

C. AWS Config only with no managed rules.

D. Amazon GuardDuty.

Answer: D
GuardDuty analyzes events such as CloudTrail management events, VPC Flow Logs, DNS logs, and S3 data events for threat detection across accounts. This is a common trap because it solves only part of the requirement: Trusted Advisor provides checks but is not a managed threat detection service for suspicious activity.

Question 9 : Design Secure Architectures

A media startup must allow analysts to query encrypted data in S3 with Athena. The KMS key policy must be least privilege. Which design is best? The solution must be suitable for production and avoid unnecessary operational risk. In this warehouse modernization, the environment includes 15,000 requests/minute; assume all services are available in the selected Region. The documented scale target is 1,117 users or events for this scenario.

A. Use SSE-KMS for the bucket and grant Athena query roles kms:Decrypt and S3 read access only to the required data locations.

B. Put the KMS key ID in the object names so Athena can discover it automatically.

C. Use SSE-S3 and give all analysts AdministratorAccess.

D. Disable encryption during Athena queries and re-enable it afterwards.

Answer: A
Athena can query SSE-KMS encrypted S3 data when the execution role has the needed S3 and KMS permissions. This is a common trap because it solves only part of the requirement: AdministratorAccess violates least privilege and SSE-S3 does not meet a requirement for customer-managed KMS access control.

Question 10 : Design Secure Architectures

A public web API is behind Amazon API Gateway. The company needs protection from common web exploits and rate-based abusive requests. Which solution should be used? The team needs the BEST answer, not merely a solution that can work. In this partner onboarding, the environment includes 6 Regions; assume all services are available in the selected Region. The documented scale target is 1,130 users or events for this scenario.

A. Place a security group directly on API Gateway and deny SQL injection payloads.

B. Associate AWS WAF with API Gateway and configure managed rule groups plus rate-based rules.

C. Use AWS Shield Advanced only and disable API Gateway throttling.

D. Create a private NAT gateway for all client requests.

Answer: B
AWS WAF integrates with API Gateway and can block common exploit patterns and rate-based traffic. The distractor is valid in another architecture but not for this scenario: Shield helps with DDoS protection, but WAF is the service used for application-layer rules such as SQL injection and rate limits.

Question 11 : Design Secure Architectures

A database on Amazon RDS must be encrypted at rest. The current DB instance is unencrypted. Which migration approach is valid? In this analytics release, the environment includes 5 PB archive; assume all services are available in the selected Region. The documented scale target is 1,143 users or events for this scenario.

A. Use a security group rule to force encrypted storage.

B. Enable encryption directly on the existing unencrypted RDS instance without downtime.

C. Attach an encrypted EBS volume to the RDS instance host.

D. Create a snapshot, copy the snapshot with encryption enabled, and restore a new encrypted DB instance from the encrypted snapshot.

Answer: D
RDS encryption for an existing unencrypted instance is commonly achieved by copying a snapshot with encryption and restoring from it. The best wrong answer is close, but it misses the stated constraint: You cannot simply toggle storage encryption on an existing unencrypted RDS instance in place.

Question 12 : Design Secure Architectures

Developers need to deploy to Amazon ECS without storing long-term AWS access keys in the CI system. The CI platform supports OIDC federation. What should the architect recommend? The current pattern has seasonal launch traffic and the team wants an AWS managed option. In this payment launch, the environment includes 2 TB; assume all services are available in the selected Region. The documented scale target is 1,156 users or events for this scenario.

A. Share the AWS account root credentials and require MFA for deployments.

B. Configure IAM OIDC federation and allow the CI identity to assume a role with scoped deployment permissions.

C. Embed temporary credentials in the container image at build time.

D. Create one IAM user with AdministratorAccess and store the access key in the CI secrets store.

Answer: B
OIDC federation lets external workloads assume IAM roles without long-term access keys. This is a common trap because it solves only part of the requirement: An IAM user access key can work technically but creates long-lived credentials and is not the preferred secure pattern.

Question 13 : Design Secure Architectures

A media startup wants to enforce encryption on every object uploaded to an S3 bucket. Uploads without encryption headers must be denied. What should be used? The architects prefer a design with minimal custom operations and clear exam-style tradeoffs. In this data platform migration, the environment includes 60 branch offices; assume all services are available in the selected Region. The documented scale target is 1,169 users or events for this scenario.

A. An S3 lifecycle rule that encrypts objects after 30 days.

B. An S3 bucket policy that denies PutObject requests missing the required server-side encryption condition.

C. A CloudFront cache policy that adds KMS permissions to viewers.

D. A security group rule that allows only port 443 to the bucket.

Answer: B
A bucket policy with encryption conditions can enforce server-side encryption at write time. The tempting wrong choice adds complexity without meeting the key requirement: Lifecycle rules do not enforce encryption at upload and would leave a gap for noncompliant objects.

Question 14 : Design Secure Architectures

A team needs private connectivity from VPC workloads to an AWS service that supports interface endpoints. Access must be limited with security groups. Which construct is appropriate? The solution must be suitable for production and avoid unnecessary operational risk. In this regional expansion, the environment includes 80 million requests/month; assume all services are available in the selected Region. The documented scale target is 1,182 users or events for this scenario.

A. Create a CloudFront distribution with signed cookies.

B. Create an internet gateway and block all public routes.

C. Create a gateway endpoint and assign it to an EC2 security group.

D. Create an AWS PrivateLink interface VPC endpoint and attach restrictive security groups.

Answer: D
Interface endpoints are elastic network interfaces in subnets and can be controlled with security groups. The distractor is valid in another architecture but not for this scenario: Gateway endpoints are route-table targets for S3 and DynamoDB and are not assigned security groups.

Question 15 : Design Secure Architectures

A customer analytics platform must store application logs centrally and detect unauthorized changes to log files. Which design is most appropriate? The team needs the BEST answer, not merely a solution that can work. In this security review, the environment includes 40 production VPCs; assume all services are available in the selected Region. The documented scale target is 1,195 users or events for this scenario.

A. Disable CloudTrail to reduce log volume and store only VPC Flow Logs.

B. Store logs only on EC2 instance volumes and rely on daily AMI backups.

C. Send logs to CloudWatch Logs and/or S3, enable log file validation for CloudTrail where applicable, and restrict write/delete access with IAM and bucket policies.

D. Give developers full S3 delete permissions so they can manage old logs manually.

Answer: C
Centralized logging with controlled access and validation supports auditability and tamper detection. The best wrong answer is close, but it misses the stated constraint: Instance-local logs can be lost if instances terminate and do not provide centralized immutable audit controls.

Question 16 : Design Secure Architectures

A retail company must secure an internet-facing application. Requirements: block common Layer 7 attacks, terminate TLS with managed certificates, and keep EC2 instances private. Which combination meets the requirements? In this performance tuning

sprint, the environment includes 300 GB/day; assume all services are available in the selected Region. The documented scale target is 1,208 users or events for this scenario.

A. Use an ALB with an ACM certificate, place instances in private subnets, and associate AWS WAF with the AL

B. B. Use S3 static website hosting for the dynamic application and attach an EBS volume.

C. Use only security groups on public instances and disable TLS at the load balancer.

D. Use a NAT gateway with an ACM certificate and put instances in public subnets.

Answer: A
ALB plus ACM plus WAF with private back-end subnets addresses TLS, application filtering, and network exposure. This is a common trap because it solves only part of the requirement: Security groups alone do not inspect Layer 7 attacks such as SQL injection or XSS.

Question 17 : Design Secure Architectures

A media startup runs a machine learning feature store in private subnets. The application must read objects from Amazon S3 without using the internet, NAT gateways, or public IP addresses. Which design should the solutions architect recommend? The current pattern has bursty event-driven traffic and the team wants an AWS managed option. In this cost review cycle, the environment includes 18 Availability Zones; assume all services are available in the selected Region. The documented scale target is 1,221 users or events for this scenario.

A. Deploy an Application Load Balancer in front of Amazon S3 and restrict it with security groups.

B. Create a gateway VPC endpoint for Amazon S3 and associate it with the private subnet route tables.

C. Attach an internet gateway to the private subnets and allow outbound HTTPS.

D. Create a NAT gateway in each Availability Zone and route S3 traffic through the NAT gateways.

Answer: B
An S3 gateway endpoint provides private S3 access from a VPC and avoids NAT gateway processing charges. The tempting wrong choice adds complexity without meeting the key requirement: NAT gateways can reach S3, but they do not satisfy the private-no-NAT requirement and add cost.

Question 18 : Design Secure Architectures

A public sector agency uses multiple AWS accounts for a IoT ingestion service. Security wants to prevent account administrators from disabling AWS CloudTrail or leaving AWS Organizations. What is the most effective control? The architects prefer a design with minimal custom operations and clear exam-style tradeoffs. In this resilience test, the environment includes 12 microservices; assume all services are available in the selected Region. The documented scale target is 1,234 users or events for this scenario.

A. Apply service control policies in AWS Organizations that deny the prohibited actions for the target OUs.

B. Use AWS WAF rules to block CloudTrail API calls.

C. Create IAM policies in each account that deny the actions to all roles except administrators.

D. Configure security groups to deny access to AWS Organizations endpoints.

Answer: A
SCPs are organization-level guardrails that restrict actions even when principals have local administrator permissions.

The tempting wrong choice adds complexity without meeting the key requirement: IAM policies inside each account are weaker because privileged local administrators can change them unless constrained by an SCP.

Question 19 : Design Secure Architectures

A partner company must upload reports to one prefix in an S3 bucket owned by a education platform. The company must not create long-term IAM users for the partner. Which approach best follows least privilege? The solution must be suitable for production and avoid unnecessary operational risk. In this audit preparation, the environment includes 25 TB; assume all services are available in the selected Region. The documented scale target is 1,247 users or events for this scenario.

A. Create an IAM user in the bucket account and email the access keys to the partner.

B. Use a security group rule that permits the partner IP range to access the bucket.

C. Use a cross-account IAM role or bucket policy that grants the partner account permission only to the required prefix.

D. Make the S3 bucket public and rely on unpredictable object names.

Answer: C
Cross-account access with a resource policy or role avoids long-term shared credentials and can be scoped to a specific prefix. This is a common trap because it solves only part of the requirement: S3 buckets are not protected by security groups, and IP-based access alone is not a full identity and least-privilege design.

Question 20 : Design Secure Architectures

A mobile app for a retail company needs user sign-up, sign-in, and temporary AWS credentials for authenticated users to access restricted resources. Which service combination should be used? The team needs the BEST answer, not merely a solution that can work. In this mobile rollout, the environment includes 200 developer accounts; assume all services are available in the selected Region. The documented scale target is 1,260 users or events for this scenario.

A. Amazon Cognito user pools and identity pools.

B. AWS Organizations accounts for every mobile user.

C. AWS IAM users for every mobile user.

D. AWS Directory Service Simple AD exposed to the internet.

Answer: A
Cognito handles application identity and can exchange authenticated identities for temporary AWS credentials. This is a common trap because it solves only part of the requirement: IAM users for app consumers create long-term credentials and do not scale securely for mobile sign-in.

Question 21 : Design Secure Architectures

A media startup stores regulated records in S3. Records must be retained for seven years and must not be deleted by any user, including administrators, during retention. What should be configured? In this warehouse modernization, the environment includes 15,000 requests/minute; assume all services are available in the selected Region. The documented scale target is 1,273 users or events for this scenario.

A. S3 Object Lock in compliance mode with an appropriate retention period.

B. S3 server access logging with MFA Delete disabled.

C. S3 Intelligent-Tiering with lifecycle expiration disabled.

D. A bucket policy that denies s3:DeleteObject to all IAM users.

Answer: A
S3 Object Lock compliance mode provides WORM retention that administrators cannot bypass during the retention period. The tempting wrong choice adds complexity without meeting the key requirement: A deny-delete bucket policy can often be changed by sufficiently privileged administrators, so it does not provide the same immutable retention.

Question 22 : Design Secure Architectures

An EC2 instance in a private subnet must retrieve database credentials securely. The team wants automatic rotation and no secrets stored in user data or environment variables. What is the best solution? The current pattern has global read traffic and the team wants an AWS managed option. In this partner onboarding, the environment includes 6 Regions; assume all services are available in the selected Region. The documented scale target is 1,286 users or events for this scenario.

A. Store the credential in AWS Secrets Manager, enable rotation, and allow the instance role to retrieve the secret.

B. Put the password in Systems Manager Parameter Store as a plain String parameter.

C. Store the password in an encrypted AMI and rotate the AMI monthly.

D. Embed the password in EC2 user data and restrict access with a security group.

Answer: A
Secrets Manager supports managed secret retrieval and rotation through IAM-controlled access. The tempting wrong choice adds complexity without meeting the key requirement: Parameter Store can store secure strings, but a plain String does not protect the secret and does not satisfy the secure-rotation requirement.

Question 23 : Design Secure Architectures

A image processing pipeline uses an Application Load Balancer. The security team requires TLS termination with managed certificates and automatic certificate renewal. What should the architect configure? The architects prefer a design with minimal custom operations and clear exam-style tradeoffs. In this analytics release, the environment includes 5 PB archive; assume all services are available in the selected Region. The documented scale target is 1,299 users or events for this scenario.

A. Upload self-signed certificates to each EC2 instance and renew them manually.

B. Use a Network ACL to encrypt traffic between clients and the load balancer.

C. Use AWS Certificate Manager certificates on the HTTPS listener of the Application Load Balancer.

D. Use AWS KMS keys directly as TLS certificates on the listener.

Answer: C
ACM integrates with ALB listeners and can renew eligible public certificates automatically. The best wrong answer is close, but it misses the stated constraint: Self-signed certificates on instances add manual operations and do not provide managed public TLS termination at the ALB.

Question 24 : Design Secure Architectures

A company needs centralized threat detection across all accounts and Regions for workloads including S3, EC2, and IAM activity. Which AWS service should be enabled with delegated administration? The solution must be suitable for production and avoid unnecessary operational risk. In this payment launch, the environment includes 2 TB; assume all services are available in the selected Region. The documented scale target is 1,312 users or events for this scenario.

A. Amazon GuardDuty.

B. AWS Trusted Advisor only.

C. Amazon Inspector only for S3 bucket policies.

D. AWS Config only with no managed rules.

Answer: A
GuardDuty analyzes events such as CloudTrail management events, VPC Flow Logs, DNS logs, and S3 data events for threat detection across accounts. The best wrong answer is close, but it misses the stated constraint: Trusted Advisor provides checks but is not a managed threat detection service for suspicious activity.

Question 25 : Design Secure Architectures

A media startup must allow analysts to query encrypted data in S3 with Athena. The KMS key policy must be least privilege. Which design is best? The team needs the BEST answer, not merely a solution that can work. In this data platform migration, the environment includes 60 branch offices; assume all services are available in the selected Region. The documented scale target is 1,325 users or events for this scenario.

A. Disable encryption during Athena queries and re-enable it afterwards.

B. Put the KMS key ID in the object names so Athena can discover it automatically.

C. Use SSE-KMS for the bucket and grant Athena query roles kms:Decrypt and S3 read access only to the required data locations.

D. Use SSE-S3 and give all analysts AdministratorAccess.

Answer: C
Athena can query SSE-KMS encrypted S3 data when the execution role has the needed S3 and KMS permissions. This is a common trap because it solves only part of the requirement: AdministratorAccess violates least privilege and SSE-S3 does not meet a requirement for customer-managed KMS access control.

Question 26 : Design Secure Architectures

A public web API is behind Amazon API Gateway. The company needs protection from common web exploits and rate-based abusive requests. Which solution should be used? In this regional expansion, the environment includes 80 million requests/month; assume all services are available in the selected Region. The documented scale target is 1,338 users or events for this scenario.

A. Place a security group directly on API Gateway and deny SQL injection payloads.

B. Use AWS Shield Advanced only and disable API Gateway throttling.

C. Create a private NAT gateway for all client requests.

D. Associate AWS WAF with API Gateway and configure managed rule groups plus rate-based rules.

Answer: D
AWS WAF integrates with API Gateway and can block common exploit patterns and rate-based traffic. The tempting wrong choice adds complexity without meeting the key requirement: Shield helps with DDoS protection, but WAF is the service used for application-layer rules such as SQL injection and rate limits.

Question 27 : Design Secure Architectures

A database on Amazon RDS must be encrypted at rest. The current DB instance is unencrypted. Which migration approach is valid? The current pattern has large month-end batches and the team wants an AWS managed option. In this security review, the environment includes 40 production VPCs; assume all services are available in the selected Region. The documented scale target is 1,351 users or events for this scenario.

A. Enable encryption directly on the existing unencrypted RDS instance without downtime.

B. Create a snapshot, copy the snapshot with encryption enabled, and restore a new encrypted DB instance from the encrypted snapshot.

C. Attach an encrypted EBS volume to the RDS instance host.

D. Use a security group rule to force encrypted storage.

Answer: B
RDS encryption for an existing unencrypted instance is commonly achieved by copying a snapshot with encryption and restoring from it. The distractor is valid in another architecture but not for this scenario: You cannot simply toggle storage encryption on an existing unencrypted RDS instance in place.

Question 28 : Design Secure Architectures

Developers need to deploy to Amazon ECS without storing long-term AWS access keys in the CI system. The CI platform supports OIDC federation. What should the architect recommend? The architects prefer a design with minimal custom operations and clear exam-style tradeoffs. In this performance tuning sprint, the environment includes 300 GB/day; assume all services are available in the selected Region. The documented scale target is 1,364 users or events for this scenario.

A. Configure IAM OIDC federation and allow the CI identity to assume a role with scoped deployment permissions.

B. Create one IAM user with AdministratorAccess and store the access key in the CI secrets store.

C. Embed temporary credentials in the container image at build time.

D. Share the AWS account root credentials and require MFA for deployments.

Answer: A
OIDC federation lets external workloads assume IAM roles without long-term access keys. The best wrong answer is close, but it misses the stated constraint: An IAM user access key can work technically but creates long-lived credentials and is not the preferred secure pattern.

Question 29 : Design Secure Architectures

A media startup wants to enforce encryption on every object uploaded to an S3 bucket. Uploads without encryption headers must be denied. What should be used? The solution must be suitable for production and avoid unnecessary operational risk. In this

cost review cycle, the environment includes 18 Availability Zones; assume all services are available in the selected Region. The documented scale target is 1,377 users or events for this scenario.

A. A security group rule that allows only port 443 to the bucket.

B. A CloudFront cache policy that adds KMS permissions to viewers.

C. An S3 lifecycle rule that encrypts objects after 30 days.

D. An S3 bucket policy that denies PutObject requests missing the required server-side encryption condition.

Answer: D
A bucket policy with encryption conditions can enforce server-side encryption at write time. The best wrong answer is close, but it misses the stated constraint: Lifecycle rules do not enforce encryption at upload and would leave a gap for noncompliant objects.

Question 30 : Design Secure Architectures

A team needs private connectivity from VPC workloads to an AWS service that supports interface endpoints. Access must be limited with security groups. Which construct is appropriate? The team needs the BEST answer, not merely a solution that can work. In this resilience test, the environment includes 12 microservices; assume all services are available in the selected Region. The documented scale target is 1,390 users or events for this scenario.

A. Create a CloudFront distribution with signed cookies.

B. Create a gateway endpoint and assign it to an EC2 security group.

C. Create an AWS PrivateLink interface VPC endpoint and attach restrictive security groups.

D. Create an internet gateway and block all public routes.

Answer: C
Interface endpoints are elastic network interfaces in subnets and can be controlled with security groups. The distractor is valid in another architecture but not for this scenario: Gateway endpoints are route-table targets for S3 and DynamoDB and are not assigned security groups.

Question 31 : Design Secure Architectures

A mobile backend must store application logs centrally and detect unauthorized changes to log files. Which design is most appropriate? In this audit preparation, the environment includes 25 TB; assume all services are available in the selected Region. The documented scale target is 1,403 users or events for this scenario.

A. Give developers full S3 delete permissions so they can manage old logs manually.

B. Send logs to CloudWatch Logs and/or S3, enable log file validation for CloudTrail where applicable, and restrict write/delete access with IAM and bucket policies.

C. Disable CloudTrail to reduce log volume and store only VPC Flow Logs.

D. Store logs only on EC2 instance volumes and rely on daily AMI backups.

Answer: B
Centralized logging with controlled access and validation supports auditability and tamper detection. The best wrong answer is close, but it misses the stated constraint: Instance-local logs can be lost if instances terminate and do not provide centralized immutable audit controls.

Question 32 : Design Secure Architectures

A retail company must secure an internet-facing application. Requirements: block common Layer 7 attacks, terminate TLS with managed certificates, and keep EC2 instances private. Which combination meets the requirements? The current pattern has steady weekday traffic and the team wants an AWS managed option. In this mobile rollout, the environment includes 200 developer accounts; assume all services are available in the selected Region. The documented scale target is 1,416 users or events for this scenario.

A. Use S3 static website hosting for the dynamic application and attach an EBS volume.

B. C. Use only security groups on public instances and disable TLS at the load balancer.

D. Use a NAT gateway with an ACM certificate and put instances in public subnets.

Answer: B
ALB plus ACM plus WAF with private back-end subnets addresses TLS, application filtering, and network exposure. The best wrong answer is close, but it misses the stated constraint: Security groups alone do not inspect Layer 7 attacks such as SQL injection or XSS.

Question 33 : Design Secure Architectures

A media startup runs a reporting system in private subnets. The application must read objects from Amazon S3 without using the internet, NAT gateways, or public IP addresses. Which design should the solutions architect recommend? The architects prefer a design with minimal custom operations and clear exam-style tradeoffs. In this warehouse modernization, the environment includes 15,000 requests/minute; assume all services are available in the selected Region. The documented scale target is 1,429 users or events for this scenario.

A. Attach an internet gateway to the private subnets and allow outbound HTTPS.

B. Deploy an Application Load Balancer in front of Amazon S3 and restrict it with security groups.

C. Create a gateway VPC endpoint for Amazon S3 and associate it with the private subnet route tables.

D. Create a NAT gateway in each Availability Zone and route S3 traffic through the NAT gateways.

Answer: C
An S3 gateway endpoint provides private S3 access from a VPC and avoids NAT gateway processing charges. The tempting wrong choice adds complexity without meeting the key requirement: NAT gateways can reach S3, but they do not satisfy the private-no-NAT requirement and add cost.

Question 34 : Design Secure Architectures

A public sector agency uses multiple AWS accounts for a order processing application. Security wants to prevent account administrators from disabling AWS CloudTrail or leaving AWS Organizations. What is the most effective control? The solution must be suitable for production and avoid unnecessary operational risk. In this partner onboarding, the environment includes 6 Regions; assume all services are available in the selected Region. The documented scale target is 1,442 users or events for this scenario.

A. Configure security groups to deny access to AWS Organizations endpoints.

B. Create IAM policies in each account that deny the actions to all roles except administrators.

C. Use AWS WAF rules to block CloudTrail API calls.

D. Apply service control policies in AWS Organizations that deny the prohibited actions for the target OUs.

Answer: D
SCPs are organization-level guardrails that restrict actions even when principals have local administrator permissions. The distractor is valid in another architecture but not for this scenario: IAM policies inside each account are weaker because privileged local administrators can change them unless constrained by an SCP.

Question 35 : Design Secure Architectures

A partner company must upload reports to one prefix in an S3 bucket owned by a education platform. The company must not create long-term IAM users for the partner. Which approach best follows least privilege? The team needs the BEST answer, not merely a solution that can work. In this analytics release, the environment includes 5 PB archive; assume all services are available in the selected Region. The documented scale target is 1,455 users or events for this scenario.

A. Make the S3 bucket public and rely on unpredictable object names.

B. Create an IAM user in the bucket account and email the access keys to the partner.

C. Use a security group rule that permits the partner IP range to access the bucket.

D. Use a cross-account IAM role or bucket policy that grants the partner account permission only to the required prefix.

Answer: D
Cross-account access with a resource policy or role avoids long-term shared credentials and can be scoped to a specific prefix. The best wrong answer is close, but it misses the stated constraint: S3 buckets are not protected by security groups, and IP-based access alone is not a full identity and least-privilege design.