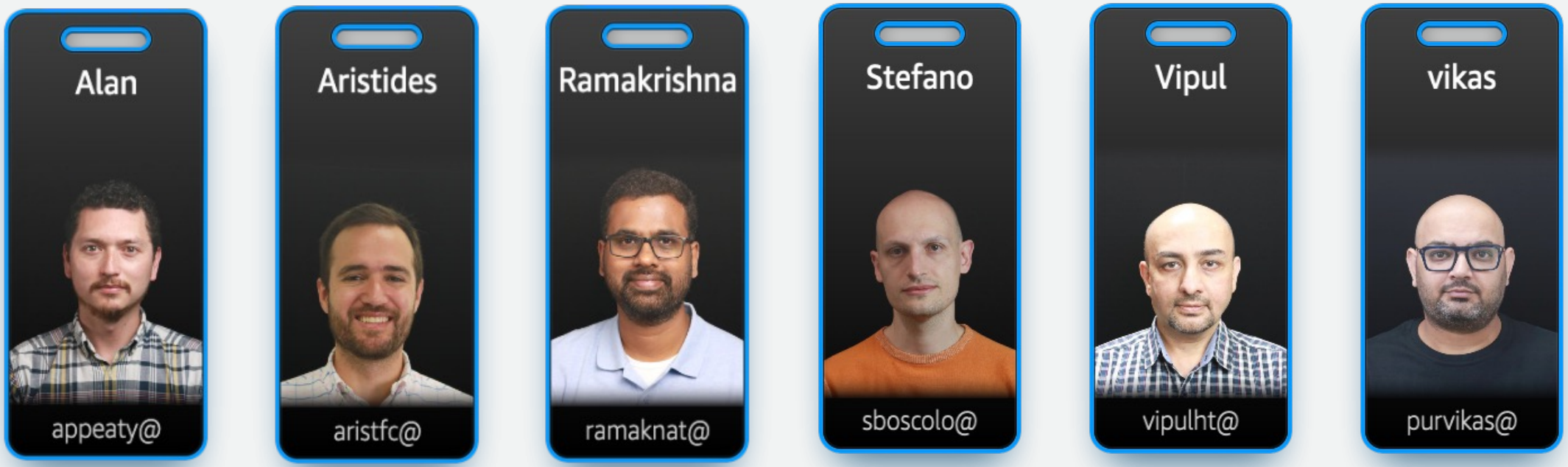
AWS Certified Solutions Architect – Associate (SAA-C03)

Exam readiness – session 1

AWS Team



Agenda

Session	Date	Topic
Session 1	15th of November 2022	• SAA-C03 exam overview • Design secure architectures
Session 2	17th of November 2022	• Differences between SAA-C02 and SAA-C03 • Design resilient architectures
Session 3	21st of November 2022	• Design high-performing architectures • design cost-optimized architectures

Today

Start (GMT)	Finish (GMT)	Topic
14:00	14:15	SAA-C03 exam overview
14:15	15:30	Practice questions and answers

Exam

Format

- 65 questions (50 are scored)
- Multiple choice or multiple response
- Minimum passing score of 720 (100-1000 scaled scoring)
- Ability to mark questions, opportunity to review them at the end
- No penalty for guessing
- Online proctor *or* testing centre
- 130 minutes duration

1.5 mins per question

review*

*Example: if you marked 30 questions for review, you have approximately 1 minute each to review them

Content

Domain	% of Exam
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%
TOTAL	**100%**

https://d1.awsstatic.com/training-and-certification/docs-sa-assoc/AWS-Certified-Solutions-Architect-Associate_Exam-Guide.pdf

What about new announcements?

"A new product, service, or feature must be generally available (GA) for 6 months prior to it appearing on a certification exam. Note that this applies only to certification exams, not training: training will cover new services and features more quickly. The AWS Certification team wants to ensure candidates have enough time to work with new services and features before they are assessed against the new material."

Where does this certificate fit?

FOUNDATIONAL

Six months of fundamental AWS Cloud and industry knowledge

PROFESSIONAL

Two years of experience designing, operating, and troubleshooting solutions using the AWS Cloud

ASSOCIATE

One year of experience solving problems and implementing solutions using the AWS Cloud

SPECIALTY

Technical AWS Cloud experience in the Specialty domain as specified in the exam guide

Q&A

Question 1

You are responsible for the administration of an Amazon VPC containing 20 Amazon EC2 instances. The VPC only contains private subnets for strict regulatory reasons. A recent application deployed into the environment requires access to an Amazon DynamoDB table. All traffic flows must remain private. Which is a valid option to facilitate this access? **[SELECT 1]**

a. Deploy a NAT Gateway.

b. Configure a resource policy for the Amazon DynamoDB table using the `aws:SourceVpc` condition.

c. Configure an Amazon VPC endpoint for Amazon DynamoDB.

d. Deploy an Internet Gateway.

e. Set up Amazon VPC peering.

Question 1

You are responsible for the administration of an Amazon VPC containing 20 Amazon EC2 instances. The VPC only contains private subnets for strict regulatory reasons. A recent application deployed into the environment requires access to an Amazon DynamoDB table. All traffic flows must remain private. Which is a valid option to facilitate this access? **[SELECT 1]**

a. Deploy a NAT Gateway.

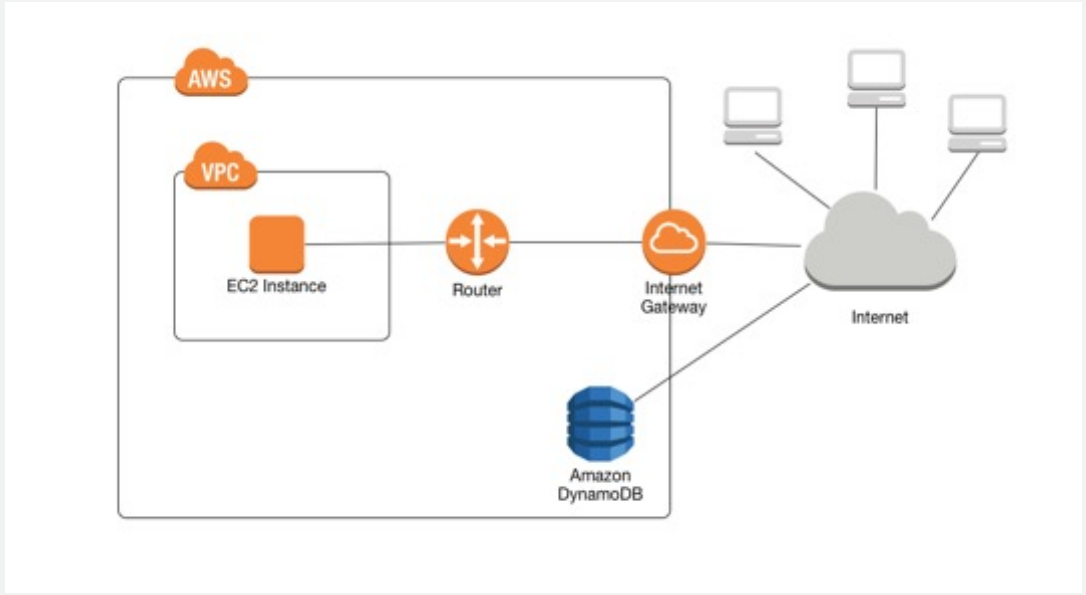
b. Configure a resource policy for the Amazon DynamoDB table using the `aws:SourceVpc` condition.

c. Configure an Amazon VPC endpoint for Amazon DynamoDB.

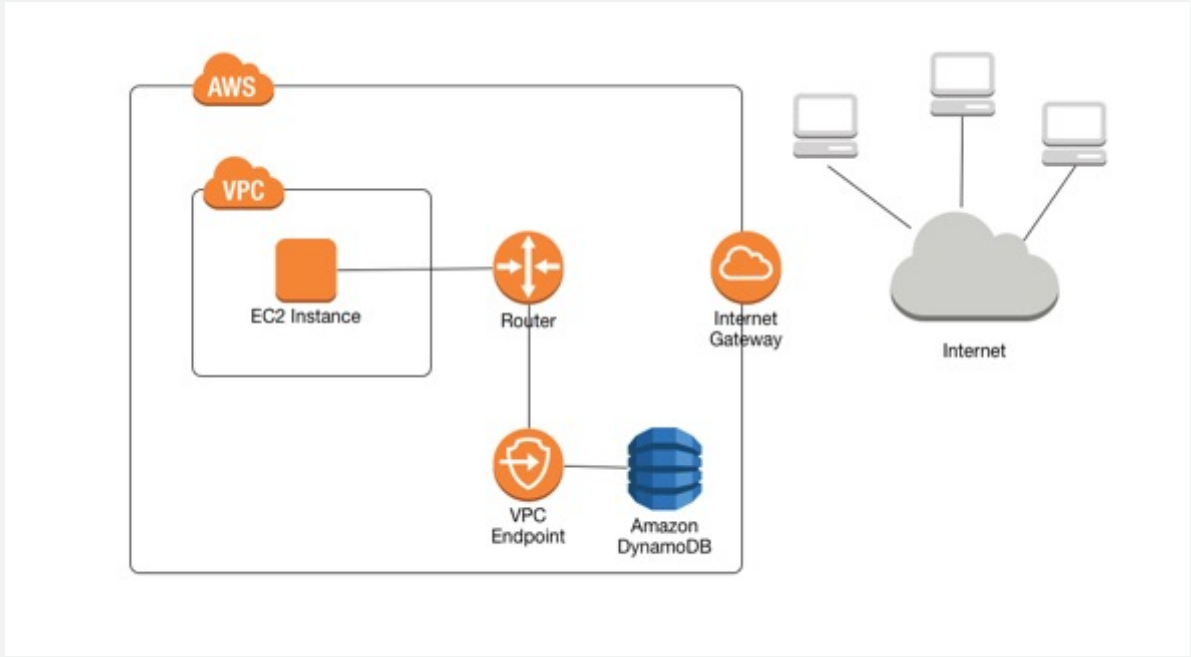
d. Deploy an Internet Gateway.

e. Set up Amazon VPC peering.

VPC endpoints



Default



VPC endpoint

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html

Question 2

Your company has developed a serverless three-tier solution for a prescription ordering service. An AWS Lambda function used to check stock levels requires read-only access to prescription records stored in an Amazon DynamoDB table. Which two actions are required to implement this securely? **[SELECT 2]**

a. Create an AWS IAM role with the necessary permissions required for the AWS Lambda function to read records from the Amazon DynamoDB table.

b. Attach the AWS IAM role to the AWS Lambda function as a resource-based policy.

c. Attach the AWS IAM role to the Amazon DynamoDB table as a resource-based policy.

d. Attach the AWS IAM role to the AWS Lambda function as an execution role.

e. Create an AWS IAM role with the necessary permissions required for the Amazon DynamoDB table to invoke the AWS Lambda function.

Question 2

Your company has developed a serverless three-tier solution for a prescription ordering service. An AWS Lambda function used to check stock levels requires read-only access to prescription records stored in an Amazon DynamoDB table. Which two actions are required to implement this securely? **[SELECT 2]**

a. Create an AWS IAM role with the necessary permissions required for the AWS Lambda function to read records from the Amazon DynamoDB table.

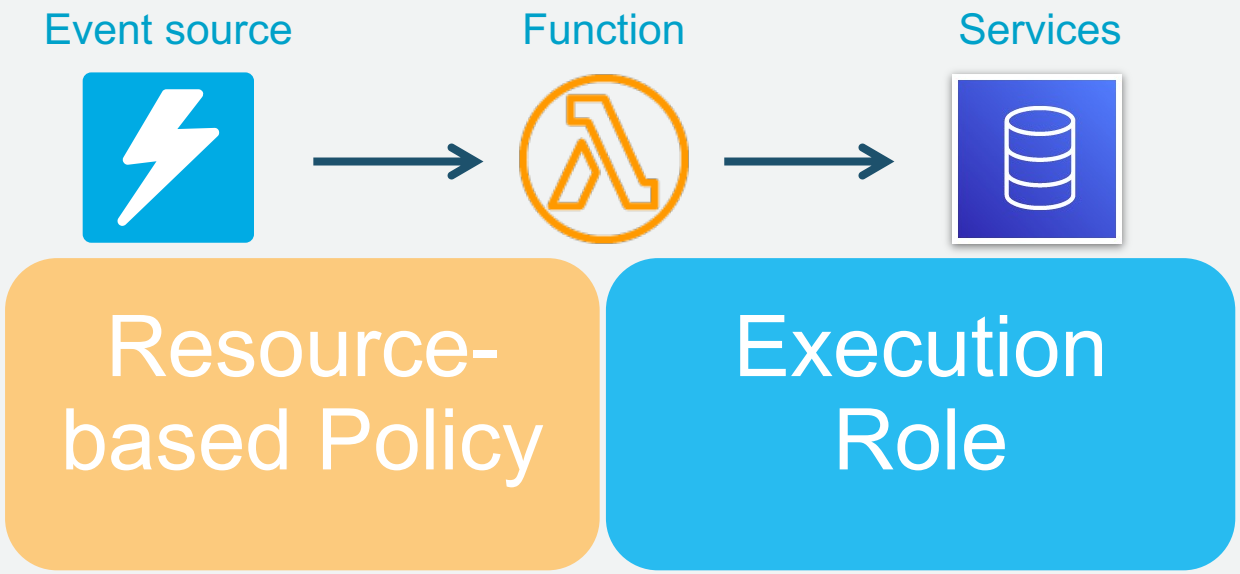
b. Attach the AWS IAM role to the AWS Lambda function as a resource-based policy.

c. Attach the AWS IAM role to the Amazon DynamoDB table as a resource-based policy.

d. Attach the AWS IAM role to the AWS Lambda function as an execution role.

e. Create an AWS IAM role with the necessary permissions required for the Amazon DynamoDB table to invoke the AWS Lambda function.

Lambda function execution role



Defines what can invoke this Lambda function

Defines what AWS resources this function can access

Example with S3 and DynamoDB:

S3 bucket *needs* to invoke a Lambda function with every PUT object (event notification). => Resource-based policy

The Lambda function *needs* to access the DynamoDB table to PUT an item. => Execution role

Question 3

A HR application running on your Amazon EC2 instance in a VPC requires read-only access to employee files stored in an Amazon S3 bucket. Which two actions are required to implement this securely? **[SELECT 2]**

a. Create an AWS IAM role with the necessary permissions required to GET objects from the Amazon S3 bucket.

b. Create a VPC security group to allow the Amazon EC2 instance access to the Amazon S3 VPC endpoint. Attach the security group to the EC2 instance.

c. Use AWS Systems Manager Parameter Store to store AWS access key ID and secret access key for an IAM user with read-only Amazon S3 permissions.

d. Attach the AWS IAM role to the Amazon EC2 instance.

Question 3

A HR application running on your Amazon EC2 instance in a VPC requires read-only access to employee files stored in an Amazon S3 bucket. Which two actions are required to implement this securely? **[SELECT 2]**

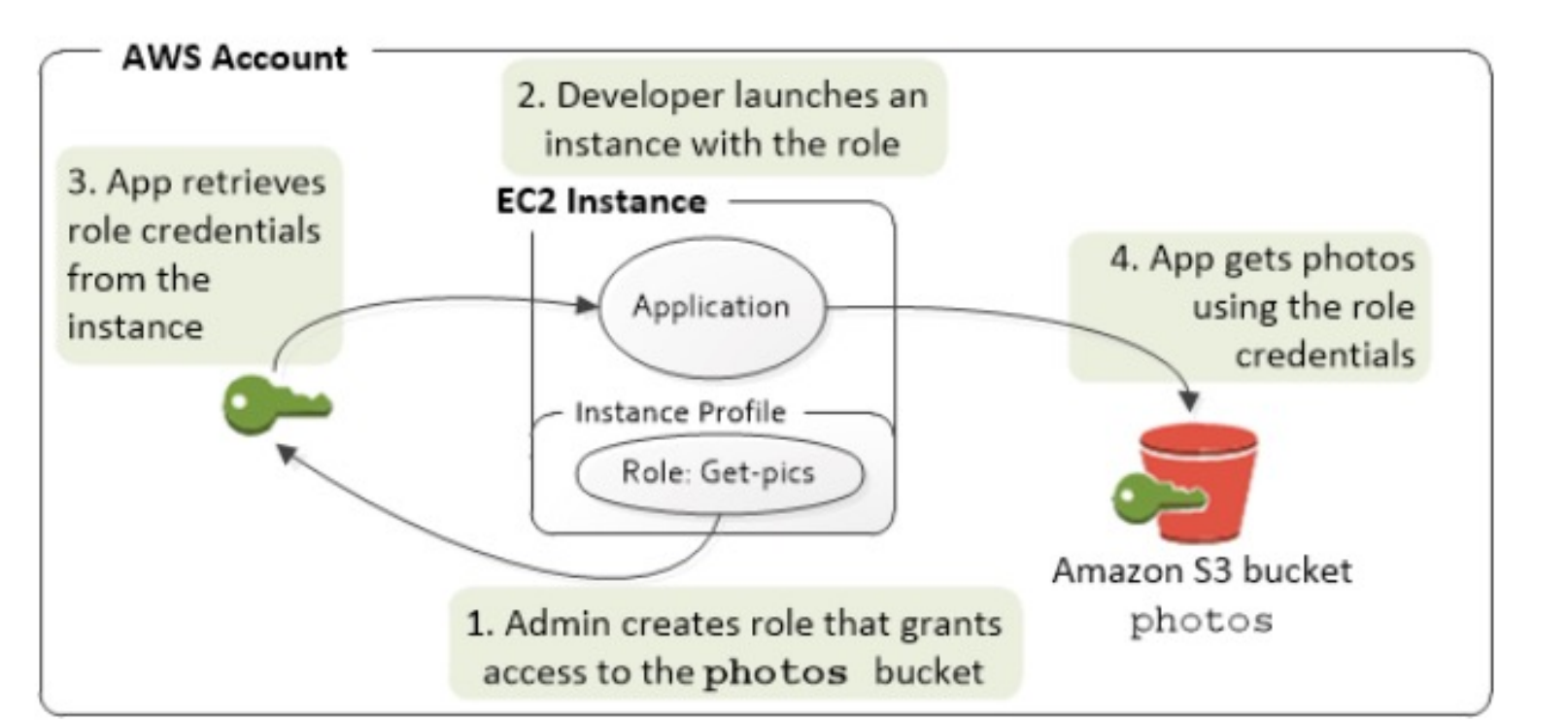
a. Create an AWS IAM role with the necessary permissions required to GET objects from the Amazon S3 bucket.

b. Create a VPC security group to allow the Amazon EC2 instance access to the Amazon S3 VPC endpoint. Attach the security group to the EC2 instance.

c. Use AWS Systems Manager Parameter Store to store AWS access key ID and secret access key for an IAM user with read-only Amazon S3 permissions.

d. Attach the AWS IAM role to the Amazon EC2 instance.

EC2 IAM roles



https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

Question 4

You work for the CIO of a motor insurance company. Recently, your competitors have reported that they were subjected to SQL injection attacks from malicious actors. The CIO would like to protect your infrastructure from similar threats. Your Amazon EC2 web servers run behind an Application Load-balancer (ALB). What should you recommend? **[SELECT 1]**

a. Enable AWS Shield Advanced and monitor CloudWatch metrics.
b. Configure Amazon GuardDuty and filter for SQL compromise findings.
c. Search for suspicious SQL statements in the ALB CloudWatch logs.
d. Enable AWS WAF on your ALB. Configure a SQL database managed rule group.
e. Enable AWS WAF on your Amazon EC2 instances. Configure a SQL database managed rule group.

Question 4

You work for the CIO of a motor insurance company. Recently, your competitors have reported that they were subjected to SQL injection attacks from malicious actors. The CIO would like to protect your infrastructure from similar threats. Your Amazon EC2 web servers run behind an Application Load-balancer (ALB). What should you recommend? **[SELECT 1]**

a. Enable AWS Shield Advanced and monitor CloudWatch metrics.

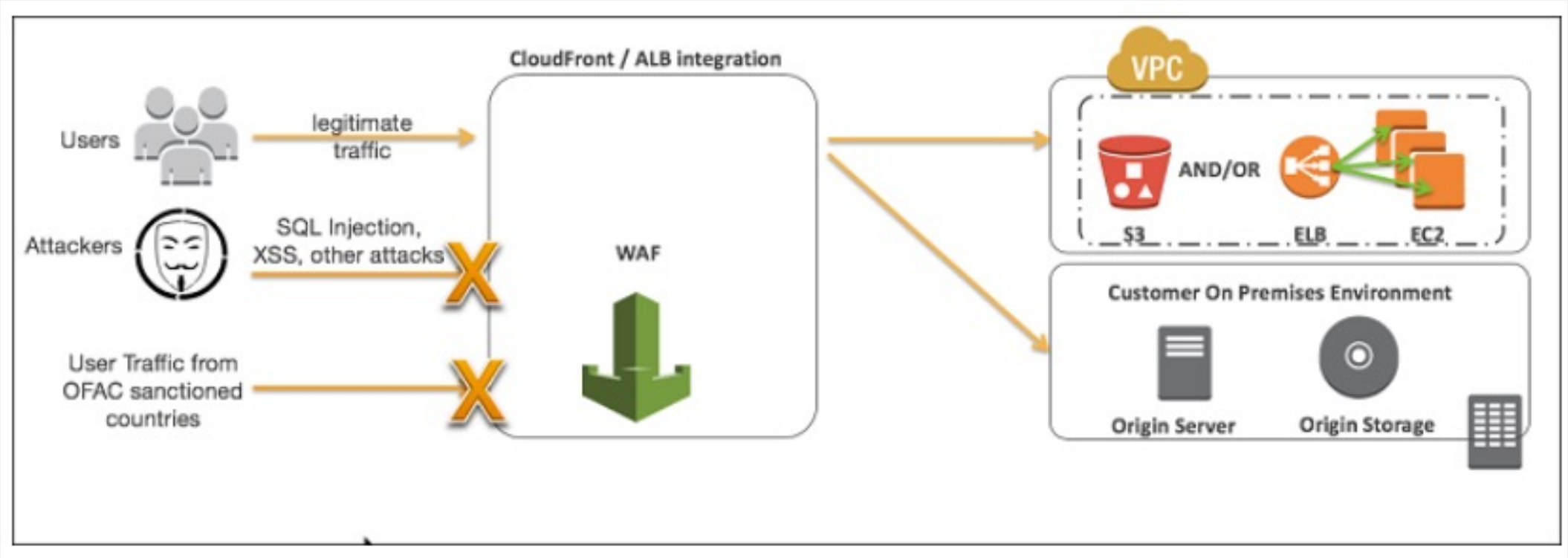
b. Configure Amazon GuardDuty and filter for SQL compromise findings.

c. Search for suspicious SQL statements in the ALB CloudWatch logs.

d. Enable AWS WAF on your ALB. Configure a SQL database managed rule group.

e. Enable AWS WAF on your Amazon EC2 instances. Configure a SQL database managed rule group.

AWS WAF



https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html

Question 5

The application engineering team has adopted a serverless-only strategy. The enterprise security team has been requested to prevent the use of Amazon EC2 instances in only the application teams' AWS accounts. Application developers however need to remain administrators of their AWS accounts. What approach would you recommend? **[SELECT 2]**

a. Set up AWS Organizations. Place AWS accounts used by the application team in the "App" Organizational Unit (OU).

b. Create an "AppAdmins" AWS IAM group. Make all application developers a member of this IAM group.

c. Apply a Service Control Policy (SCP) denying Amazon EC2 permissions on the "App" OU.

d. Apply a policy denying Amazon EC2 permissions to the "AppAdmins" AWS IAM group.

Question 5

The application engineering team has adopted a serverless-only strategy. The enterprise security team has been requested to prevent the use of Amazon EC2 instances in only the application teams' AWS accounts. Application developers however need to remain administrators of their AWS accounts. What approach would you recommend? **[SELECT 2]**

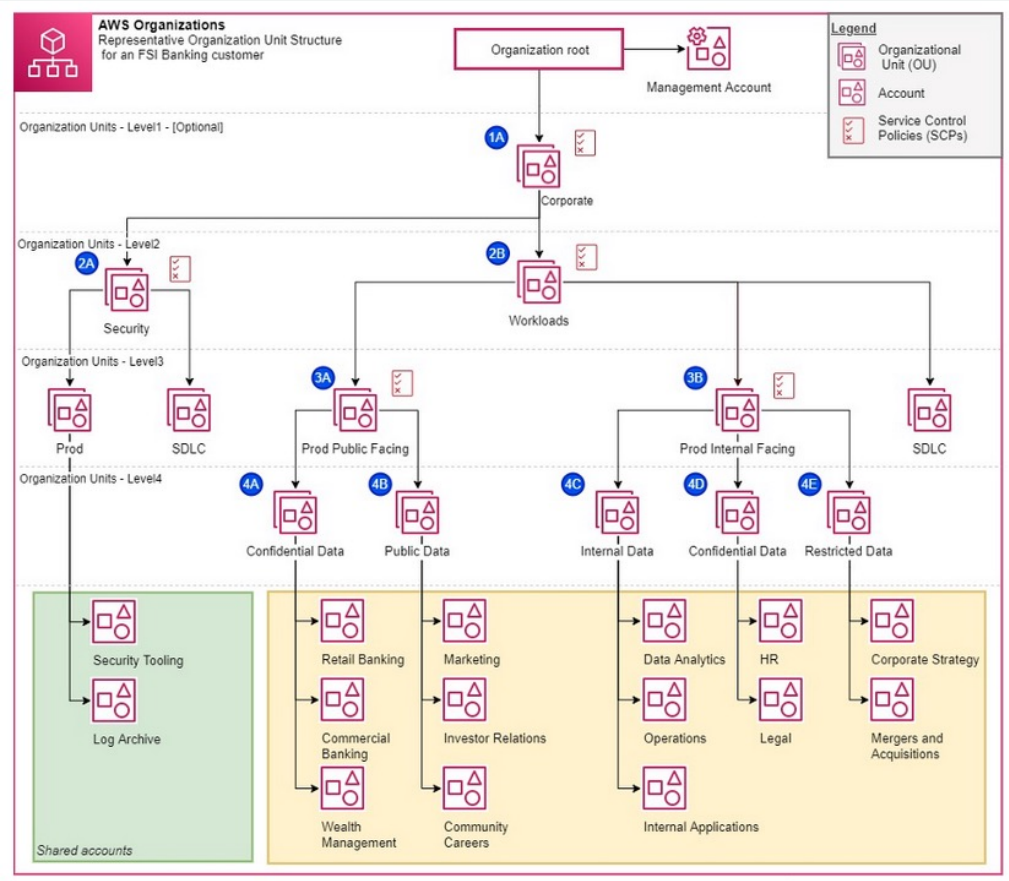
a. Set up AWS Organizations. Place AWS accounts used by the application team in the "App" Organizational Unit (OU).

b. Create an "AppAdmins" AWS IAM group. Make all application developers a member of this IAM group.

c. Apply a Security Control Policy (SCP) denying Amazon EC2 permissions on the "App" OU.

d. Apply a policy denying Amazon EC2 permissions to the "AppAdmins" AWS IAM group.

Service control policies



https://aws.amazon.com/blogs/industries/best-practices-for-aws-organizations-service-control-policies-in-a-multi-account-environment/

Question 6

Your application consists of web servers running on two Amazon EC2 instances, and a MySQL database running on another EC2 instance. The two web servers must be load-balanced for high availability. All EC2 instances need to be able to connect to the internet to download patches. What is the most secure way to deploy this architecture? **[SELECT 2]**

a. Locate all EC2 instances in private subnets. Route 0.0.0.0/0 traffic to an Internet Gateway (IGW) from the private subnets.

b. Locate all EC2 instances in private subnets. Route 0.0.0.0/0 traffic to NAT Gateways (NGWs) from the private subnets.

c. Associate an internet-facing Elastic Load-Balancer (ELB) to the public subnets. Load-balance web server EC2 instances in the private subnets.

d. Associate an internet-facing Elastic Load-Balancer (ELB) to the private subnets. Load-balance web server EC2 instances in the private subnets.

Question 6

Your application consists of web servers running on two Amazon EC2 instances, and a MySQL database running on another EC2 instance. The two web servers must be load-balanced for high availability. All EC2 instances need to be able to connect to the internet to download patches. What is the most secure way to deploy this architecture? **[SELECT 2]**

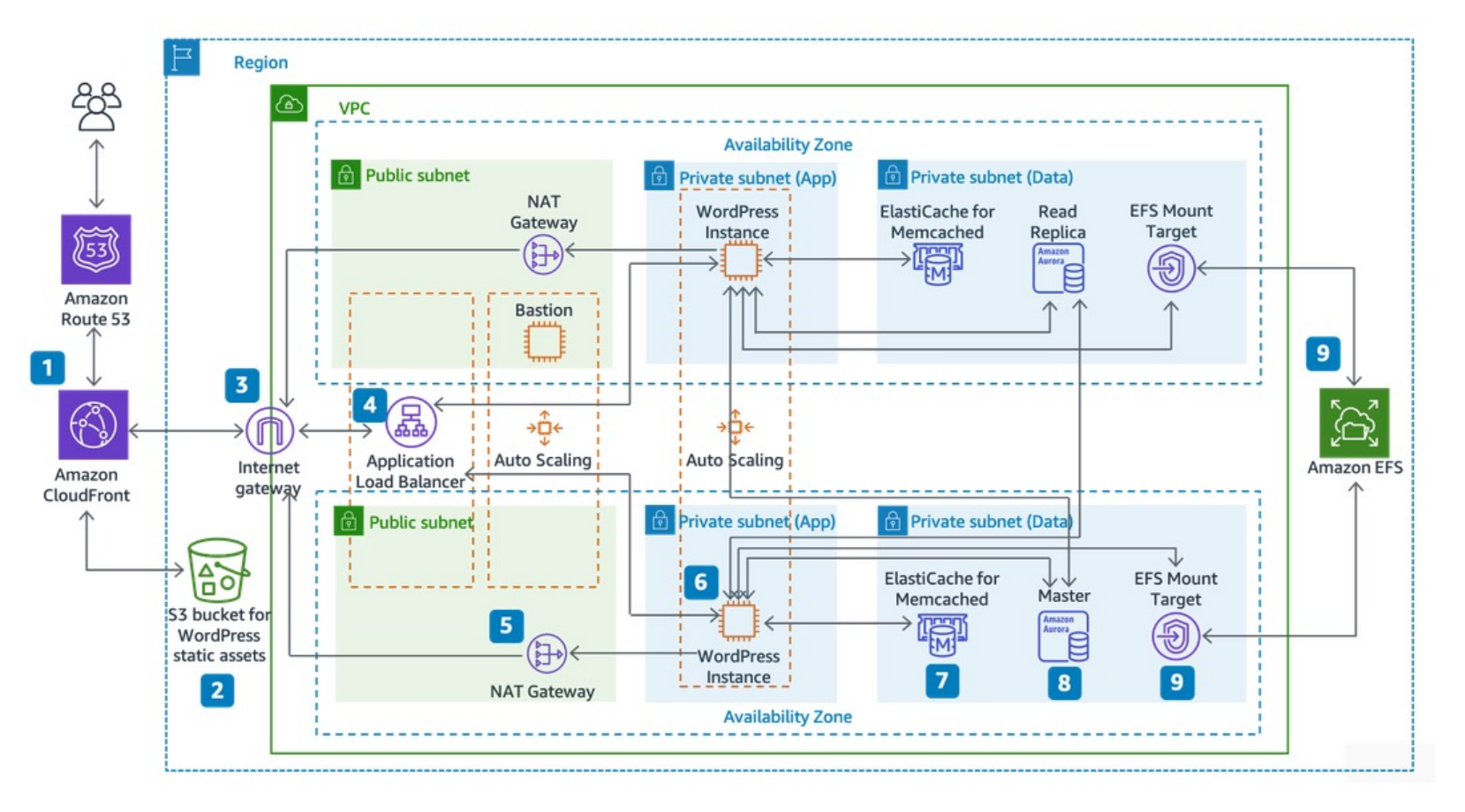
a. Locate all EC2 instances in private subnets. Route 0.0.0.0/0 traffic to an Internet Gateway (IGW) from the private subnets.

b. Locate all EC2 instances in private subnets. Route 0.0.0.0/0 traffic to NAT Gateways (NGWs) from the private subnets.

c. Associate an internet-facing Elastic Load-Balancer (ELB) to the public subnets. Load-balance web server EC2 instances in the private subnets.

d. Associate an internet-facing Elastic Load-Balancer (ELB) to the private subnets. Load-balance web server EC2 instances in the private subnets.

WordPress on AWS example



https://docs.aws.amazon.com/whitepapers/latest/best-practices-wordpress/reference-architecture.html

Question 7

You must ensure that AWS API calls are collected across all company AWS accounts, are preserved online, and are instantly available for analysis for 90 days. For compliance reasons, this data must also be restorable for 7 years. What is the most efficient way to meet this requirement? **[SELECT 1]**

a. Configure Amazon CloudWatch Logs across all accounts to export API logs to an Amazon S3 bucket. Set a S3 lifecycle policy to move the data to S3 Glacier after 90 days, and expire the data after 7 years.

b. Enable AWS CloudTrail logging across all accounts. Extend the CloudTrail retention policy to 7 years.

c. Configure Amazon CloudWatch Logs across all accounts to stream API logs to an Amazon S3 bucket with S3 Intelligent-Tiering configured.

d. Enable AWS CloudTrail logging across all accounts to a centralised Amazon S3 bucket. Set a S3 lifecycle policy to move the data to Glacier after 90 days, and expire the data after 7 years.

Question 7

You must ensure that AWS API calls are collected across all company AWS accounts, are preserved online, and are instantly available for analysis for 90 days. For compliance reasons, this data must also be restorable for 7 years. What is the most efficient way to meet this requirement? **[SELECT 1]**

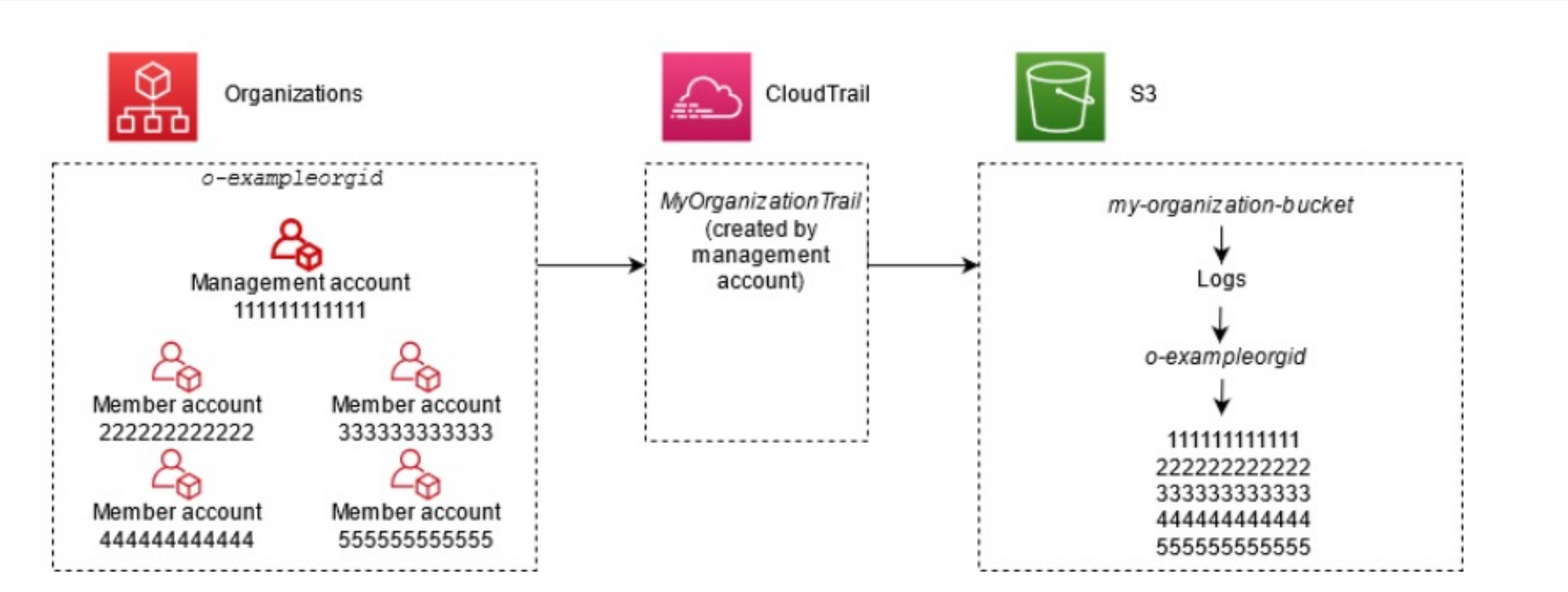
a. Configure Amazon CloudWatch Logs across all accounts to export API logs to an Amazon S3 bucket. Set a S3 lifecycle policy to move the data to S3 Glacier after 90 days, and expire the data after 7 years.

b. Enable AWS CloudTrail logging across all accounts. Extend the CloudTrail retention policy to 7 years.

c. Configure Amazon CloudWatch Logs across all accounts to stream API logs to an Amazon S3 bucket with S3 Intelligent-Tiering configured.

d. Enable AWS CloudTrail logging across all accounts to a centralised Amazon S3 bucket. Set a S3 lifecycle policy to move the data to Glacier after 90 days, and expire the data after 7 years.

AWS Organizations and AWS CloudTrail



https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html

Question 8

A company's security team requires that Amazon S3 encrypts your objects before saving them on disks in AWS data centers, and decrypts them when you download the objects. The encryption process should be managed by Amazon S3. Which S3 encryption options would best meet this requirement? **[SELECT 2]**

a. Amazon S3-managed keys (SSE-S3)

b. AWS Encryption SDK

c. Amazon Key Management Service key (SSE-KMS)

d. Use gpg -c <file> and gpg -d <file> commands

Question 8

A company's security team requires that Amazon S3 encrypts your objects before saving them on disks in AWS data centers, and decrypts them when you download the objects. The encryption process should be managed by Amazon S3. Which S3 encryption options would best meet this requirement? **[SELECT 2]**

a. Amazon S3-managed keys (SSE-S3)

b. AWS Encryption SDK

c. Amazon Key Management Service key (SSE-KMS)

d. Use gpg -c <file> and gpg -d <file> commands

S3 data encryption

Protecting data using encryption

PDF | RSS

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit using Secure Socket Layer/Transport Layer Security (SSL/TLS) or client-side encryption. You have the following options for protecting data at rest in Amazon S3:

- **Server-Side Encryption** – Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects.

  To configure server-side encryption, see Specifying server-side encryption with AWS KMS (SSE-KMS) or Specifying Amazon S3 encryption.
- **Client-Side Encryption** – Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

  To configure client-side encryption, see Protecting data using client-side encryption.

For more information about server-side encryption and client-side encryption, review the topics listed below.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html

Question 9

You have recently created a new Amazon VPC security group to provide the application running on an Amazon EC2 instance access to a MySQL database running on another EC2 instance. They both reside in the same private subnet. However, you notice that it is not possible to establish a connection to the database from the application. What could be the potential issue? **[SELECT 1]**

a. There is a deny rule in the new security group.

b. There is no allow rule in the new security group.

c. The new security group has an outbound rule to the “database” EC2 instance. However, in the same security group, you have not created an inbound rule in the opposite direction for the return traffic.

d. Subnet has a NACL attached. By default, a NACL denies all inbound and outbound traffic.

Question 9

You have recently created a new Amazon VPC security group to provide the application running on an Amazon EC2 instance access to a MySQL database running on another EC2 instance. They both reside in the same private subnet. However, you notice that it is not possible to establish a connection to the database from the application. What could be the potential issue? **[SELECT 1]**

a. There is a deny rule in the new security group.

b. There is no allow rule in the new security group.

c. The new security group has an outbound rule to the “database” EC2 instance. However, in the same security group, you have not created an inbound rule in the opposite direction for the return traffic.

d. Subnet has a NACL attached. By default, a NACL denies all inbound and outbound traffic.

Security Group vs NACL

Compare security groups and network ACLs

The following table summarizes the basic differences between security groups and network ACLs.

Security group	Network ACL
Operates at the instance level	Operates at the subnet level
Applies to an instance only if it is associated with the instance	Applies to all instances deployed in the associated subnet (providing an additional layer of defense if security group rules are too permissive)
Supports allow rules only	Supports allow rules and deny rules
We evaluate all rules before deciding whether to allow traffic	We evaluate rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic
Stateful: Return traffic is allowed, regardless of the rules	Stateless: Return traffic must be explicitly allowed by rules

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html

Question 10

You are trying to detect if an Amazon VPC security group or network access control list (NACL) are blocking traffic from one Amazon EC2 instance to another. You have exhausted all troubleshooting options on the EC2 instances themselves and you now want to monitor ongoing traffic flow between the elastic network interfaces. Which tool would allow you to do this with the least configuration? **[SELECT 1]**

a. Amazon Route 53 logs
b. Amazon VPC traffic mirroring
c. Amazon VPC reachability analyzer
d. Amazon VPC flow logs

Question 10

You are trying to detect if an Amazon VPC security group or network access control list (NACL) are blocking traffic from one Amazon EC2 instance to another. You have exhausted all troubleshooting options on the EC2 instances themselves and you now want to monitor ongoing traffic flow between the elastic network interfaces. Which tool would allow you to do this with the least configuration? **[SELECT 1]**

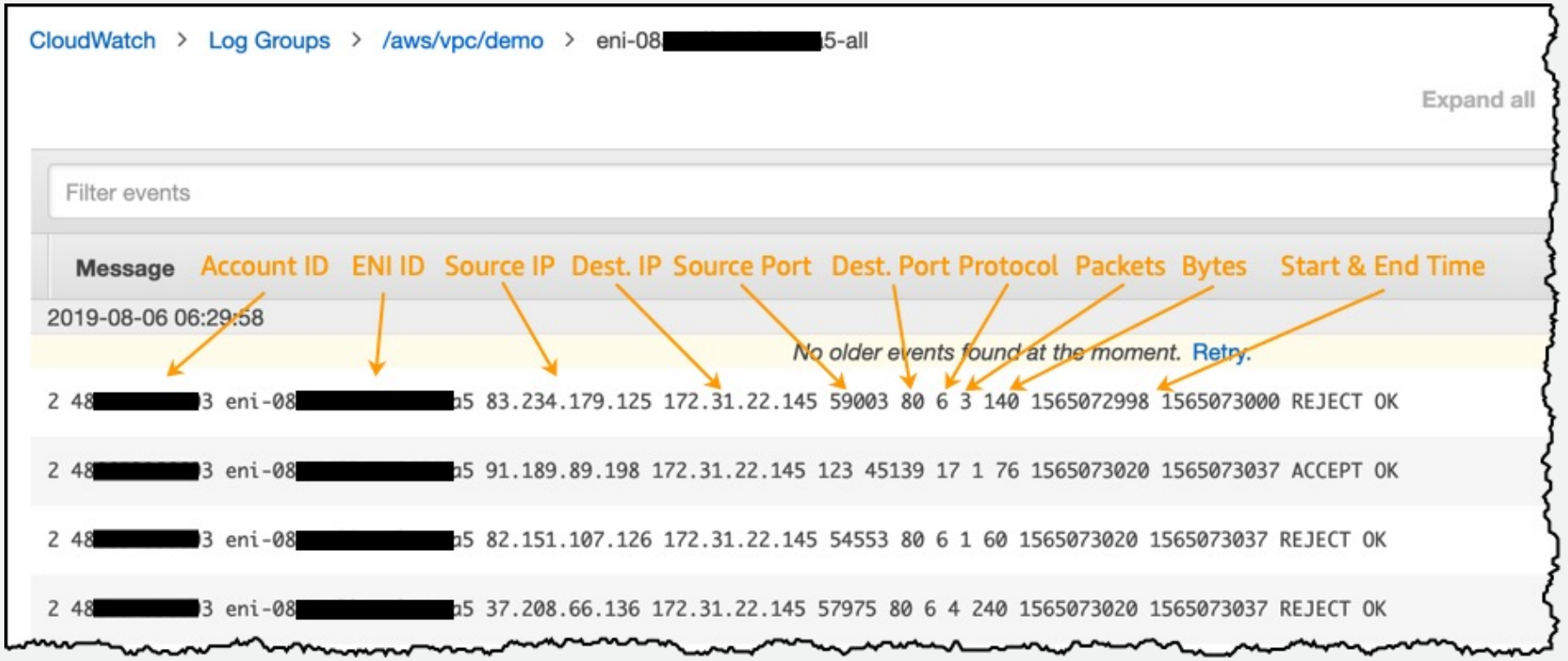
a. Amazon Route 53 logs

b. Amazon VPC traffic mirroring

c. Amazon VPC reachability analyzer

d. Amazon VPC flow logs

VPC Flow Logs



https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html

Join us on the next session!

Session	Date	Topic
~~Session 1~~	~~15th of November 2022~~	~~• SAA-C03 exam overview~~ ~~• Design secure architectures~~
Session 2	17th of November 2022	• Differences between SAA-C02 and SAA-C03 • Design resilient architectures
Session 3	21st of November 2022	• Design high-performing architectures • design cost-optimized architectures

Survey

Thank you!