SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/scs-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A Development team has built an experimental environment to test a simple stale web application It has built an isolated VPC with a private and a public subnet. The public subnet holds only an Application Load Balancer a NAT gateway, and an internet gateway. The private subnet holds ail of the Amazon EC2 instances

There are 3 different types of servers Each server type has its own Security Group that limits access lo only required connectivity. The Security Groups nave both inbound and outbound rules applied Each subnet has both inbound and outbound network ACIs applied to limit access to only required connectivity

Which of the following should the team check if a server cannot establish an outbound connection to the internet? (Select THREE.)

A. The route tables and the outbound rules on the appropriate private subnet security group

B. The outbound network ACL rules on the private subnet and the Inbound network ACL rules on the public subnet

C. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet

D. The rules on any host-based firewall that may be applied on the Amazon EC2 instances

E. The Security Group applied to the Application Load Balancer and NAT gateway

F. That the 0.0.0./0 route in the private subnet route table points to the internet gateway in the public subnet

Correct Answer: CEF

because these are the factors that could affect the outbound connection to the internet from a server in a private subnet. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet must allow the traffic to pass through. The security group applied to the application load balancer and NAT gateway must also allow the traffic from the private subnet. The 0.0.0.0/0 route in the private subnet route table must point to the NAT gateway in the public subnet, not the internet gateway. The other options are either irrelevant or incorrect for troubleshooting the outbound connection issue.

QUESTION 2

A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted The security engineer has configured the integration of IAM CloudTrail with Amazon CloudWatch

What should the security engineer do next to meet this requirement?

A. Use inbound rule 100 to allow traffic on TCP port 443 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443

B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port

C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port

D. Use inbound rule 100 to deny traffic on TCP port 3306 Use inbound rule 200 to allow traffic on TCP port 443 Use

outbound rule 100 to allow traffic on TCP port 443

Correct Answer: A

QUESTION 3

A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.

Which solution will meet these requirements with the LEAST management overhead?

A. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use identity-based policies to restrict access to which IAM principals can access the images.

B. Pull images from the public container registry. Publish the images to a private container registry that is hosted on Amazon EC2 instances in a centralized AWS account. Deploy host-based container scanning tools to EC2 instances that run Amazon ECS. Restrict access to the container images by using basic authentication over HTTPS.

C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

D. Pull images from the public container registry. Publish the images to AWS CodeArtifact repositories in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

Correct Answer: C

The correct answer is C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline

to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

This solution meets the requirements because:

Amazon ECR is a fully managed container registry service that supports Docker and OCI images and artifacts. It integrates with Amazon ECS and other AWS services to simplify the development and deployment of container-based

applications.

Amazon ECR provides image scanning on push, which uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project to detect software vulnerabilities in container images. The scan results are

available in the AWS Management Console, AWS CLI, or AWS SDKs. Amazon ECR supports cross-account access to repositories, which allows sharing images across multiple AWS accounts3. This can be achieved by using repository

policies, which are resource-based policies that specify which IAM principals and accounts can access the repositories and what actions they can perform4. Additionally, identity-based policies can be used to control which IAM roles in each

account can access the repositories.

The other options are incorrect because:

A. This option does not use repository policies to restrict cross-account access to the images, which is a requirement. Identity-based policies alone are not sufficient to control access to Amazon ECR repositories. B. This option does not use Amazon ECR, which is a fully managed service that provides image scanning and cross-account access features. Hosting a private container registry on EC2 instances would require more management overhead and additional security measures.

D. This option uses AWS CodeArtifact, which is a fully managed artifact repository service that supports Maven, npm, NuGet, PyPI, and generic package formats However, AWS CodeArtifact does not support Docker or OCI container images, which are required for Amazon ECS applications.

QUESTION 4

A security engineer is configuring account-based access control (ABAC) to allow only specific principals to put objects into an Amazon S3 bucket. The principals already have access to Amazon S3.

The security engineer needs to configure a bucket policy that allows principals to put objects into the S3 bucket only if the value of the Team tag on the object matches the value of the Team tag that is associated with the principal. During testing, the security engineer notices that a principal can still put objects into the S3 bucket when the tag values do not match.

Which combination of factors are causing the PutObject operation to succeed when the tag values are different? (Select TWO.)

A. The principal\\'s identity-based policy grants access to put objects into the S3 bucket with no conditions.

B. The principal\\'s identity-based policy overrides the condition because the identity-based policy contains an explicit allow.

C. The S3 bucket\\'s resource policy does not deny access to put objects.

D. The S3 bucket\\'s resource policy cannot allow actions to the principal.

E. The bucket policy does not apply to principals in the same zone of trust.

Correct Answer: AC

When using ABAC, the principal\\'s identity-based policy and the S3 bucket\\'s resource policy are both evaluated to determine the effective permissions. If either policy grants access to the principal, the action is allowed. If either policy denies access to the principal, the action is denied. Therefore, to enforce the tag-based condition, both policies must deny access when the tag values do not match. In this case, the principal\\'s identity-based policy grants access to put objects into the S3 bucket with no conditions (A), which means that the policy does not check for the tag values. This policy overrides the condition in the bucket policy because an explicit allow always takes precedence over an implicit deny. The bucket policy can only allow or deny actions to the principal based on the condition, but it cannot override the identity-based policy. The S3 bucket\\'s resource policy does not deny access to put objects ? which means that it also does not check for the tag values. The bucket policy can only allow or deny actions to the principal based on the condition, but it cannot override the identity-based policy. Therefore, the combination of factors A and C are causing the PutObject operation to succeed when the tag values are different. References: Using ABAC with Amazon S3 Bucket policy examples

QUESTION 5

A recent security audit found that IAM CloudTrail logs are insufficiently protected from tampering and unauthorized access Which actions must the Security Engineer take to address these audit findings? (Select THREE)

A. Ensure CloudTrail log file validation is turned on

B. Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long-term storage

C. Use an S3 bucket with tight access controls that exists m a separate account

D. Use Amazon Inspector to monitor the file integrity of CloudTrail log files.

E. Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files

F. Encrypt the CloudTrail log files with server-side encryption with IAM KMS-managed keys (SSE-KMS)

Correct Answer: ADE