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 company plans to create individual child accounts within an existing organization in IAM Organizations for each of its DevOps teams. IAM CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized IAM account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.

How can the security engineer meet these requirements?

A. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the IAM account root user.

B. Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the IAM account root user in the source account.

C. Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.

D. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new IAM group. Have team members use individual IAM accounts that are members of the new IAM group.

Correct Answer: D

QUESTION 2

A company\\'s Security Engineer has been asked to monitor and report all IAM account root user activities.

Which of the following would enable the Security Engineer to monitor and report all root user activities? (Select TWO)

A. Configuring IAM Organizations to monitor root user API calls on the paying account

B. Creating an Amazon CloudWatch Events rule that will trigger when any API call from the root user is reported

C. Configuring Amazon Inspector to scan the IAM account for any root user activity

D. Configuring IAM Trusted Advisor to send an email to the Security team when the root user logs in to the console

E. Using Amazon SNS to notify the target group

Correct Answer: BE

QUESTION 3

An ecommerce company is developing new architecture for an application release. The company needs to implement TLS for incoming traffic to the application. Traffic for the application will originate from the internet TLS does not have to be implemented in an end- to-end configuration because the company is concerned about impacts on performance. The incoming traffic types will be HTTP and HTTPS The application uses ports 80 and 443.

What should a security engineer do to meet these requirements?

A. Create a public Application Load Balancer. Create two listeners one listener on port 80 and one listener on port 443.

Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443 Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 443.

B. Create a public Application Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443 Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 80.

C. Create a public Network Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443. Set the protocol for the listener on port 443 to TLS.

D. Create a public Network Load Balancer. Create a listener on port 443. Create one target group. Create a rule to forward traffic from port 443 to the target group. Set the protocol for the listener on port 443 to TLS.

Correct Answer: A

An Application Load Balancer (ALB) is a type of load balancer that operates at the application layer (layer 7) of the OSI model. It can distribute incoming traffic based on the content of the request, such as the host header, path, or query

parameters. An ALB can also terminate TLS connections and decrypt requests from clients before sending them to the targets.

To implement TLS for incoming traffic to the application, the following steps are required:

Create a public ALB in a public subnet and register the EC2 instances as targets in a target group.

Create two listeners for the ALB, one on port 80 for HTTP traffic and one on port 443 for HTTPS traffic.

Create a rule for the listener on port 80 to redirect HTTP requests to HTTPS using the same host, path, and query parameters.

Provision a public TLS certificate in AWS Certificate Manager (ACM) for the domain name of the application. ACM is a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS

services and your internal connected resources.

Attach the certificate to the listener on port 443 and configure the security policy to negotiate secure connections between clients and the ALB. Configure the security groups for the ALB and the EC2 instances to allow inbound traffic on ports

80 and 443 from the internet and outbound traffic on any port to the EC2 instances.

This solution will meet the requirements of implementing TLS for incoming traffic without impacting performance or requiring end-to-end encryption. The ALB will handle the TLS termination and decryption, while forwarding unencrypted

requests to the EC2 instances.

Verified References:

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.h tml

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https- listener.html

https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

QUESTION 4

A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator\\'s workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below

Please select:

A. Port 443 coming from 0.0.0.0/0

B. Port 443 coming from 10.0.0.0/16

C. Port 22 coming from 0.0.0.0/0

D. Port 22 coming from 203.0.113.1/32

Correct Answer: AD

Explanation: Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet. Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk For more information on IAM Security Groups, please visit the following UR https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-secunty.htmll The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

QUESTION 5

A company manages three separate IAM accounts for its production, development, and test environments, Each Developer is assigned a unique IAM user under the development account. A new application hosted on an Amazon EC2 instance in the developer account requires read access to the archived documents stored in an Amazon S3 bucket in the production account.

How should access be granted?

A. Create an IAM role in the production account and allow EC2 instances in the development account to assume that role using the trust policy. Provide read access for the required S3 bucket to this role.

B. Use a custom identity broker to allow Developer IAM users to temporarily access the S3 bucket.

C. Create a temporary IAM user for the application to use in the production account.

D. Create a temporary IAM user in the production account and provide read access to Amazon S3. Generate the temporary IAM user\\'s access key and secret key and store these on the EC2 instance used by the application in the development account.

Correct Answer: A

Explanation: https://IAM.amazon.com/premiumsupport/knowledge-center/cross-account- access-s3/