SCS-C01 Q&As

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

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

https://www.passapply.com/aws-certified-security-specialty.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 maintains sensitive data in an Amazon S3 bucket that must be protected using an AWS KMS CMK. The company requires that keys be rotated automatically every year.

How should the bucket be configured?

A. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select an AWS-managed CMK.

B. Select Amazon S3-AWS KMS managed encryption keys (S3-KMS) and select a customer-managed CMK with key rotation enabled.

C. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select a customer-managed CMK that has imported key material.

D. Select server-side encryption with AWS KMS-managed keys (SSE-KMS) and select an alias to an AWS-managed CMK.

Correct Answer: B

QUESTION 2

A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.

Which application flow would meet the data protection requirements on AWS?

A. Digitized files -> Amazon Kinesis Data Analytics

B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena

C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena

D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Correct Answer: B

QUESTION 3

A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these AWS CloudTrail log events. The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the Analyst perform?

A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst\\'s AWS account.

B. Verify that a metric filter was created and then mapped to an alarm. Check the alarm notification action.

C. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for

security group changes.

D. Verify that the Analyst\\'s account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Correct Answer: B

MetricFilter:

Type: \\'AWS::Logs::MetricFilter\\'

Properties:

LogGroupName: \\'\\'

FilterPattern: >{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) ||

($.eventName =

RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName =

CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) } MetricTransformations:

-MetricValue: \\'1\\' MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

QUESTION 4

An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            <Action>
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
            ]
            <CONDITION>
        }
    ]
}
```


What additional items need to be added to the IAM user policy? (Choose two.)

A. kms:GenerateDataKey

B. kms:Decrypt

C. kms:CreateGrant

D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonaws.com"}}

E. "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}

Correct Answer: CE

The EBS which is AWS resource service is encrypted with CMK and to allow EC2 to decrypt , the IAM user should create a grant (action) and a boolean condition for the AWs resource . This link explains how AWS keys works. https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

QUESTION 5

Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don\\'t have any critical security flaws. Which of the following can be done to ensure this? Choose 2 answers from the options given below.

Please select:

A. Use AWS Config to ensure that the servers have no critical flaws.

B. Use AWS inspector to ensure that the servers have no critical flaws.

C. Use AWS inspector to patch the servers

D. Use AWS SSM to patch the servers

Correct Answer: BD

The AWS Documentation mentions the following on AWS Inspector Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API. Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers Option C is invalid because the AWS Inspector service is not used to patch servers For more information on AWS Inspector, please visit the following URL: https://aws.amazon.com/inspector> Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool. For more information on the Systems Manager, please visit the following URL: https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html The correct answers are: Use AWS Inspector to ensure that the servers have no critical flaws.. Use AWS SSM to patch the servers

QUESTION 6

A company uses multiple AWS accounts managed with AWS Organizations. Security engineers have created a standard set of security groups for all these. accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only.

A recent security audit found that the security groups are inconsistently implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.

Which solution should the security engineer recommend?

A. Use AWS Resource Access Manager to create shared resources for each required security group and apply an IAM policy that permits read-only access to the security groups only.

B. Create an AWS CloudFormation template that creates the required security groups Execute the template as part of configuring new accounts Enable Amazon Simple Notification Service (Amazon SNS) notifications when changes occur

C. Use AWS Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation

D. Use AWS Control Tower to edit the account factory template to enable the snare security groups option Apply an SCP to the OU or individual accounts that prohibits security group modifications from local account users

Correct Answer: A

QUESTION 7

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.

Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below

Please select:

A. A network ACL with a rule that allows outgoing traffic on port 443.

B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports

C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

D. A security group with a rule that allows outgoing traffic on port 443

E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports.

F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Correct Answer: BD

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port. Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not required For more information on VPC Security Groups, please visit the below URL: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.htmll The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group

with a rule that allows outgoing traffic on port 443

QUESTION 8

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

A. Associate the instances to the same security groups.

B. Add 0.0.0.0/0 to the egress rules of the instance security groups.

C. Add the instance IDs to the ingress rules of the instance security groups.

D. Add the public IP addresses to the ingress rules of the instance security groups.

Correct Answer: D

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules- reference.html#sg-rulesother-instances

QUESTION 9

A company uses a third-party identity provider and SAML-based SSO for its AWS accounts After the thirdparty identity provider renewed an expired signing certificate users saw the following message when trying to log in:

A security engineer needs to provide a solution that corrects the error and minimizes operational overhead Which solution meets these requirements?

A. Upload the third-party signing certificate\\'s new private key to the AWS identity provider entity defined in AWS identity and Access Management (IAM) by using the AWS Management Console

B. Sign the identity provider\\'s metadata file with the new public key Upload the signature to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI.

C. Download the updated SAML metadata tile from the identity service provider Update the file in the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI

D. Configure the AWS identity provider entity defined in AWS Identity and Access Management (IAM) to synchronously fetch the new public key by using the AWS Management Console.

Correct Answer: C

QUESTION 10

Users report intermittent availability of a web application hosted on AWS. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier.

Which of the following techniques will improve the availability of the application? (Choose two.)

A. Deploy AWS WAF to block all unsecured web applications from accessing the internet.

B. Deploy an Intrusion Detection/Prevention System (IDS/IPS) to monitor or block unusual incoming network traffic.

C. Configure security groups to allow outgoing network traffic only from hosts that are protected with upto-date antivirus software.

D. Create Amazon CloudFront distribution and configure AWS WAF rules to protect the web applications from malicious traffic.

E. Use the default Amazon VPC for externakfacing systems to allow AWS to actively block malicious network traffic affecting Amazon EC2 instances.

Correct Answer: AB

QUESTION 11

An auditor needs access to logs that record all API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below Please select:

A. Configure the CloudTrail service in each AWS account, and have the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary IAM account that can assume a read- only role in the secondary AWS accounts.

B. Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary accounts. Then grant the auditor access to the S3 bucket that receives the CloudTrail log files.

C. Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.

D. Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and erant the auditor access to that single bucket in the orimarv account.

Correct Answer: D

Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of AWS resources as possibli AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting only be granted access in one location Option A is incorrect since the auditor should B is incorrect since consolidated billing is not a key requirement as part of the question Option C is incorrect since there is not consolidated logging For more information on Cloudtrail please refer to the below URL: https://aws.amazon.com/cloudtraiL The correct answer is: Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bud in the primary account and grant the auditor access to that single bucket in the primary account.

QUESTION 12

A Security Engineer is working with a Product team building a web application on AWS. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.

Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

A. Create a custom authorization service using AWS Lambda.

B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.

C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.

D. Configure an Amazon Cognito identity pool to integrate with social login providers.

E. Update DynamoDB to store the user email addresses and passwords.

F. Update API Gateway to use a COGNITO_USER_POOLS authorizer.

Correct Answer: BDE