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.pass4itsure.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 Security Engineer received an AWS Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.

Which action should the Engineer take based on this situation? (Choose three.)

A. Use AWS Artifact to capture an exact image of the state of each instance.

B. Create EBS Snapshots of each of the volumes attached to the compromised instances.

C. Capture a memory dump.

D. Log in to each instance with administrative credentials to restart the instance.

E. Revoke all network ingress and egress except for to/from a forensics workstation.

F. Run Auto Recovery for Amazon EC2.

Correct Answer: BEF

QUESTION 2

A Security Engineer is troubleshooting an issue with a company\\'s custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events lo an Amazon SNS topic. All logs are encrypted at rest using an AWS KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.

The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No togs are being received.

What should the Security Engineer do to troubleshoot this issue?

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
   {
    "Sid": "Access-to-specific-VPCE-only",
    "Principal": "*",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": ["arn:aws:s3:::examplebucket",
            "arn:aws:s3:::examplebucket/*"],
    "Condition": {
     "StringNotEquals": {
      "aws:sourceVpce": "vpce-1a2b3c4d"
     }
    }
   }
  ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 3

A company has five AWS accounts and wants to use AWS CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.

Which of the following steps will implement these requirements? (Choose three.)

A. Create a new S3 bucket in a separate AWS account for centralized storage of CloudTrail logs, and enable "Log File Validation" on all trails.

B. Use an existing S3 bucket in one of the accounts, apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3: PutObject" action and the "s3 GetBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.

C. Apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3 PutObject" action and the "s3 GelBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.

D. Use unique log file prefixes for trails in each AWS account.

E. Configure CloudTrail in the centralized account to log all accounts to the new centralized S3 bucket.

F. Enable encryption of the log files by using AWS Key Management Service

Correct Answer: ACE

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html

If you have created an organization in AWS Organizations, you can create a trail that will log all events for all AWS accounts in that organization. This is sometimes referred to as an organization trail. You can also choose to edit an existing trail in the master account and apply it to an organization, making it an organization trail. Organization trails log events for the master account and all member accounts in the organization. For more information about AWS Organizations, see Organizations Terminology and Concepts. Note Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html You must be logged in with the master account for the organization in order to create an organization trail. You must also have sufficient permissions for the IAM user or role in the master account in order to successfully create an organization trail. If you do not have sufficient permissions, you will not see the option to apply a trail to an organization.

QUESTION 4

Which of the following is not a best practice for carrying out a security audit?

Please select:

A. Conduct an audit on a yearly basis

B. Conduct an audit if application instances have been added to your account

C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account

D. Whenever there are changes in your organization

Correct Answer: A

A year\\'s time is generally too long a gap for conducting security audits The AWS Documentation mentions the following

You should audit your security configuration in the following situations:

On a periodic basis.

If there are changes in your organization, such as people leaving. If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need. If you\\'ve added

or

removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWor stacks, AWS CloudFormation templates, etc. If you ever suspect that an unauthorized person might have accessed your account. Option B,

C and D are all the right ways and recommended best practices when it comes to conducting audits For more information on Security Audit guideline, please visit the below URL:

https://docs.aws.amazon.com/eeneral/latest/gr/aws-security-audit-euide.html

The correct answer is: Conduct an audit on a yearly basis

QUESTION 5

Your company has a set of EC2 Instances defined in AWS. These Ec2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly. How can you achieve this?

Please select:

A. Use Cloudwatch logs to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS for the notification.

B. Use Cloudwatch metrics to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS for the notification.

C. Use AWS inspector to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS f the notification.

D. Use Cloudwatch events to be triggered for any changes to the Security Groups.Configure the Lambda function for email notification as well.

Correct Answer: D

The below diagram from an AWS blog shows how security groups can be monitored Option A is invalid because you need to use Cloudwatch Events to check for chan, Option B is invalid because you need to use Cloudwatch Events to check for chang Option C is invalid because AWS inspector is not used to monitor the activity on Security Groups For more information on monitoring security groups, please visit the below URL: Ihttpsy/aws.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notifications-about-changes-to-your-amazonj \\'pc-security-groups/ The correct answer is: Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:Put*",
            "Resource":"arn:aws:s3:::centralizedbucket/*",
            "Effect": "Deny"
        },
        {
            "Action": ["s3:Get*","s3:List*"],
            "Resource": [
                "arn:aws:s3:::centralizedbucket/*",
                "arn:aws:s3:::centralizedbucket/"
            ],
            "Effect": "Allow"
        ]
    ]
}
```