SCS-C01^{Q&As}

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

QUESTION 1

A company finds that one of its Amazon EC2 instances suddenly has a high CPU usage. The company does not know whether the EC2 instance is compromised or whether the operating system is performing background cleanup.

Which combination of steps should a security engineer take before investigating the issue? (Choose three.)

A. Disable termination protection for the EC2 instance if termination protection has not been disabled.

B. Enable termination protection for the EC2 instance if termination protection has not been enabled.

C. Take snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.

D. Remove all snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.

E. Capture the EC2 instance metadata, and then tag the EC2 instance as under quarantine.

F. Immediately remove any entries in the EC2 instance metadata that contain sensitive information.

Correct Answer: ABF

QUESTION 2

A company has a requirement that no Amazon EC2 security group can allow SSH access from the CIDR block 0.0.0.0/0. The company wants to monitor compliance with this requirement at all times and wants to receive a near-real-time notification if any security group is noncompliant.

A security engineer has configured AWS Config and will use the restricted-ssh managed rule to monitor the security groups.

What should the security engineer do next to meet these requirements?

A. Configure AWS Config to send its configuration snapshots to an Amazon S3 bucket. Create an AWS Lambda function to run on a PutEvent to the S3 bucket. Configure the Lambda function to parse the snapshot for a compliance change to the restricted-ssh managed rule. Configure the Lambda function to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic if a change is discovered.

B. Configure an Amazon EventBridge (Amazon CloudWatch Events) event rule that is invoked by a compliance change event from AWS Config for the restricted-ssh managed rule. Configure the event rule to target an Amazon Simple Notification Service (Amazon SNS) topic that will provide a notification.

C. Configure AWS Config to push all its compliance notifications to Amazon CloudWatch Logs. Configure a CloudWatch Logs metric filter on the AWS Config log group to look for a compliance notification change on the restricted-ssh managed rule. Create an Amazon CloudWatch alarm on the metric filter to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic if the alarm is in the ALARM state.

D. Configure an Amazon CloudWatch alarm on the CloudWatch metric for the restricted-ssh managed rule. Configure the CloudWatch alarm to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic if the alarm is in the ALARM state.

Correct Answer: A

QUESTION 3

You have been given a new brief from your supervisor for a client who needs a web application set up on AWS. The a most important requirement is that MySQL must be used as the database, and this database must not be hosted in t? public cloud, but rather at the client\\'s data center due to security risks. Which of the following solutions would be the ^ best to assure that the client\\'s requirements are met? Choose the correct answer from the options below

Please select:

A. Build the application server on a public subnet and the database at the client\\'s data center. Connect them with a VPN connection which uses IPsec.

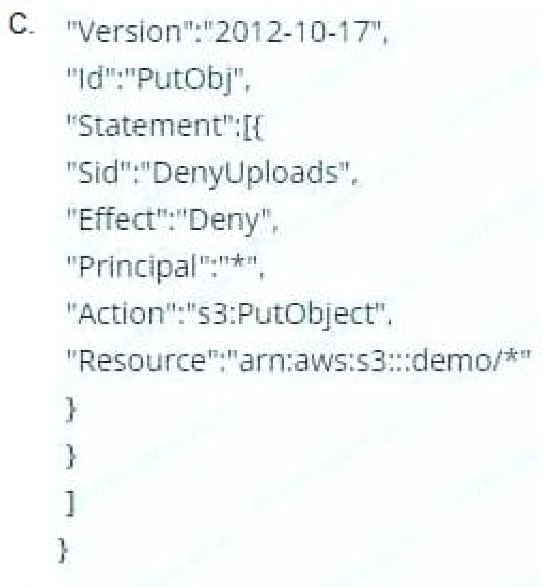
B. Use the public subnet for the application server and use RDS with a storage gateway to access and synchronize the data securely from the local data center.

C. Build the application server on a public subnet and the database on a private subnet with a NAT instance between them.

D. Build the application server on a public subnet and build the database in a private subnet with a secure ssh connection to the private subnet from the client\\'s data center.

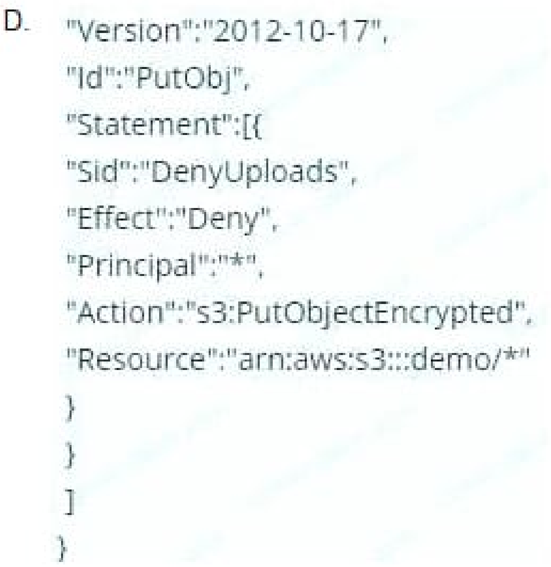
Correct Answer: A

Since the database should not be hosted on the cloud all other options are invalid. The best option is to create a VPN connection for securing traffic as shown below.



C.

```
 "Version":"2012-10-17",
 "Id":"PutObj",
 "Statement":[{
 "Sid":"DenyUploads",
 "Effect":"Deny",
 "Principal":"*",
 "Action":"s3:PutObject",
 "Resource":"arn:aws:s3:::demo/*"
 }
 }
 ]
}
```



D.

```
 "Version":"2012-10-17",
 "Id":"PutObj",
 "Statement":[{
 "Sid":"DenyUploads",
 "Effect":"Deny",
 "Principal":"*",
 "Action":"s3:PutObjectEncrypted",
 "Resource":"arn:aws:s3:::demo/*"
 }
 }
 ]
}
```

Option B is invalid because this is the incorrect use of the Storage gateway Option C is invalid since this is the incorrect use of the NAT instance Option D is invalid since this is an incorrect configuration For more information on VPN connections, please visit the below URL http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.htmll The correct answer is: Build the application server on a public subnet and the database at the client\\'s data center. Connect them with a VPN connection which uses IPsec

QUESTION 4

A company deployed Amazon GuardDuty in the us-east-1 Region. The company wants all DNS logs that relate to the company\\'s Amazon EC2 instances to be inspected. What should a security engineer do to ensure that the EC2 instances are logged?

A. Use IPv6 addresses that are configured for hostnames.

B. Configure external DNS resolvers as internal resolvers that are visible only to AWS.

C. Use AWS DNS resolvers for all EC2 instances.

D. Configure a third-party DNS resolver with logging for all EC2 instances.

Correct Answer: C

Reference: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html

QUESTION 5

A company has Windows Amazon EC2 instances in a VPC that are joined to on-premises Active Directory servers for domain services. The security team has enabled Amazon GuardDuty on the AWS account to alert on issues with the

instances.

During a weekly audit of network traffic, the Security Engineer notices that one of the EC2 instances is attempting to communicate with a known command-and-control server but failing. This alert does not show up in GuardDuty.

Why did GuardDuty fail to alert to this behavior?

A. GuardDuty did not have the appropriate alerts activated.

B. GuardDuty does not see these DNS requests.

C. GuardDuty only monitors active network traffic flow for command-and-control activity.

D. GuardDuty does not report on command-and-control activity.

Correct Answer: B

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_backdoor.html