

# Exam Questions SCS-C01

AWS Certified Security- Specialty

<https://www.2passeasy.com/dumps/SCS-C01/>



#### NEW QUESTION 1

- (Exam Topic 1)

A company has several workloads running on AWS. Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet but currently, there is no authentication system built into the application.

How should the Security Engineer implement employee-only access to this system without changing the application?

- A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication (or the ALB). Define a SAML-based Amazon Cognito user pool and connect it to ADFS. Implement AWS SSO in the master account and link it to ADFS as an identity provider. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.
- B. Define an Amazon Cognito identity pool, then install the connector on the Active Directory server. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their
- C. Active Directory user names and passwords.
- D. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2. Ensure the security group on Amazon EC2 only allows access from the Lambda function.

**Answer: B**

#### NEW QUESTION 2

- (Exam Topic 1)

A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:

- A trusted forensic environment must be provisioned
- Automated response processes must be orchestrated

Which AWS services should be included in the plan? (Select TWO)

- A. AWS CloudFormation
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. Amazon Macie
- E. AWS Step Functions

**Answer: AE**

#### NEW QUESTION 3

- (Exam Topic 1)

A company wants to encrypt the private network between its on-premises environment and AWS. The company also wants a consistent network experience for its employees.

What should the company do to meet these requirements?

- A. Establish an AWS Direct Connect connection with AWS and set up a Direct Connect gateway.
- B. In the Direct Connect gateway configuration, enable IPsec and BGP, and then leverage native AWS network encryption between Availability Zones and Regions.
- C. Establish an AWS Direct Connect connection with AWS and set up a Direct Connect gateway.
- D. Using the Direct Connect gateway, create a private virtual interface and advertise the customer gateway private IP address.
- E. Create a VPN connection using the customer gateway and the virtual private gateway.
- F. Establish a VPN connection with the AWS virtual private cloud over the internet.
- G. Establish an AWS Direct Connect connection with AWS and establish a public virtual interface.
- H. For prefixes that need to be advertised, enter the customer gateway public IP address.
- I. Create a VPN connection over Direct Connect using the customer gateway and the virtual private gateway.

**Answer: C**

#### NEW QUESTION 4

- (Exam Topic 1)

A company wants to encrypt data locally while meeting regulatory requirements related to key exhaustion. The encryption key can be no more than 10 days old or encrypt more than 2<sup>16</sup> objects. Any encryption key must be generated on a FIPS-validated hardware security module (HSM). The company is cost-conscious, as plans to upload an average of 100 objects to Amazon S3 each second for sustained operations across 5 data producers.

When approach MOST efficiently meets the company's needs?

- A. Use the AWS Encryption SDK and set the maximum age to 10 days and the minimum number of messages encrypted to 2<sup>16</sup>. Use AWS Key Management Service (AWS KMS) to generate the master key and data key. Use data key caching with the Encryption SDK during the encryption process.
- B. Use AWS Key Management Service (AWS KMS) to generate an AWS managed CMK.
- C. Then use Amazon S3 client-side encryption configured to automatically rotate with every object.
- D. Use AWS CloudHSM to generate the master key and data key.
- E. Then use Boto 3 and Python to locally encrypt data before uploading the object. Rotate the data key every 10 days or after 2<sup>16</sup> objects have been uploaded to Amazon S3.
- F. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) and set the master key to automatically rotate.

**Answer: A**

#### NEW QUESTION 5

- (Exam Topic 1)

A company has hundreds of AWS accounts, and a centralized Amazon S3 bucket used to collect AWS CloudTrail logs for all of these accounts. A security engineer wants to create a solution that will enable the company to run ad hoc queries against its CloudTrail logs dating back 3 years from when the trails were first enabled in the company's AWS account.

How should the company accomplish this with the least amount of administrative overhead?

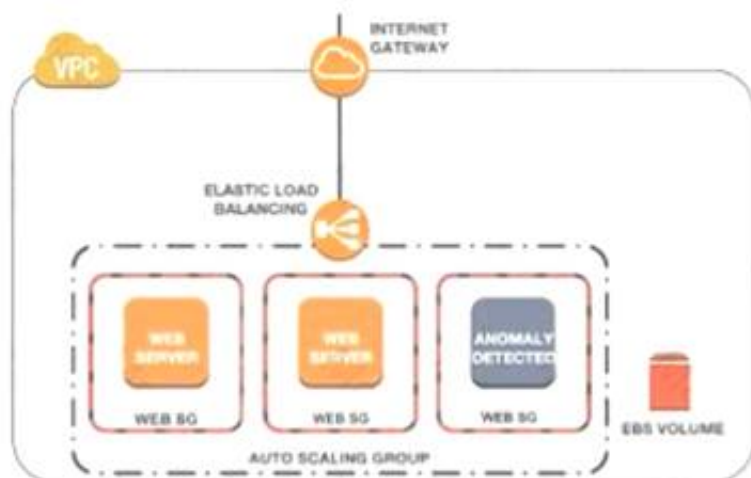
- A. Run an Amazon EMP cluster that uses a MapReduce job to be examine the CloudTrail trails.
- B. Use the events history/feature of the CloudTrail console to query the CloudTrail trails.
- C. Write an AWS Lambda function to query the CloudTrail trails Configure the Lambda function to be executed whenever a new file is created in the CloudTrail S3 bucket.
- D. Create an Amazon Athena table that tools at the S3 bucket the CloudTrail trails are being written to Use Athena to run queries against the trails.

**Answer: D**

#### NEW QUESTION 6

- (Exam Topic 1)

A Security Engineer noticed an anomaly within a company EC2 instance as shown in the image. The Engineer must now investigate what e causing the anomaly. What are the MOST effective steps to take lo ensure that the instance is not further manipulated while allowing the Engineer to understand what happened?



- A. Remove the instance from the Auto Scaling group Place the instance within an isolation security group, detach the EBS volume launch an EC2 instance with a forensic toolkit and attach the E8S volume to investigate
- B. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, launch an EC2 instance with a forensic toolkit, and allow the forensic toolkit image to connect to the suspicious Instance to perform the Investigation.
- C. Remove the instance from the Auto Scaling group Place the Instance within an isolation security group, launch an EC2 Instance with a forensic toolkit and use the forensic toolkit imago to deploy an ENI as a network span port to inspect all traffic coming from the suspicious instance.
- D. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, make a copy of the EBS volume from a new snapshot, launch an EC2 Instance with a forensic toolkit and attach the copy of the EBS volume to investigate.

**Answer: B**

#### NEW QUESTION 7

- (Exam Topic 1)

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

- A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.
- B. Move the web servers to private subnets without public IP addresses.
- C. Configure AWS WAF to provide DDoS attack protection for the ALB.
- D. Require all inbound network traffic to route through a bastion host in the private subnet.
- E. Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

**Answer: BC**

#### NEW QUESTION 8

- (Exam Topic 1)

A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application

Which combination of actions would provide the MOST secure solution? (Select TWO )

- A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances
- B. Enable AWS WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances
- C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs
- D. Create a usage plan Generate a set of API keys for each application that needs to call the API.
- E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

**Answer: AE**

#### NEW QUESTION 9

- (Exam Topic 1)

A Security Engineer is setting up a new AWS account. The Engineer has been asked to continuously monitor the company's AWS account using automated compliance checks based on AWS best practices and Center for Internet Security (CIS) AWS Foundations Benchmarks

How can the Security Engineer accomplish this using AWS services?

- A. Enable AWS Config and set it to record all resources in all Regions and global resource
- B. Then enable AWS Security Hub and confirm that the CIS AWS Foundations compliance standard is enabled
- C. Enable Amazon Inspector and configure it to scan all Regions for the CIS AWS Foundations Benchmark

- D. Then enable AWS Security Hub and configure it to ingest the Amazon Inspector findings
- E. Enable Amazon Inspector and configure it to scan all Regions for the CIS AWS Foundations Benchmark
- F. Then enable AWS Shield in all Regions to protect the account from DDoS attacks.
- G. Enable AWS Config and set it to record all resources in all Regions and global resources Then enable Amazon Inspector and configure it to enforce CIS AWS Foundations Benchmarks using AWS Config rules.

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 1)

A company's information security team wants to analyze Amazon EC2 performance and utilization data in the near-real time for anomalies. A Sec Engineer is responsible for log aggregation. The Engineer must collect logs from all of the company's AWS accounts in centralized location to perform the analysis.

How should the Security Engineer do this?

Log in to each account four te a day and filter the AWS CloudTrail log data, then copy and paste the logs in to the Amazon S3 bucket in the destination account.

- A. Set up Amazon CloudWatch to stream data to an Amazon S3 bucket in each source account
- B. Set up bucket replication for each source account into a centralized bucket owned by the security Engineer.
- C. Set up an AWS Config aggregator to collect AWS configuration data from multiple sources.
- D. Set up an AWS config aggregator to collect AWS configuration data from multiple sources.
- E. Set up Amazon CloudWatch cross-account log data sharing with subscriptions in each account
- F. Send the logs to Amazon Kinesis Data Firehose in the Security Engineer's account.

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 1)

A security engineer is auditing a production system and discovers several additional IAM roles that are not required and were not previously documented during the last audit 90 days ago. The engineer is trying to find out who created these IAM roles and when they were created. The solution must have the lowest operational overhead.

Which solution will meet this requirement?

- A. Import AWS CloudTrail logs from Amazon S3 into an Amazon Elasticsearch Service cluster, and search through the combined logs for CreateRole events.
- B. Create a table in Amazon Athena for AWS CloudTrail event
- C. Query the table in Amazon Athena for CreateRole events.
- D. Use AWS Config to look up the configuration timeline for the additional IAM roles and view the linked AWS CloudTrail event.
- E. Download the credentials report from the IAM console to view the details for each IAM entity, including the creation dates.

**Answer:** A

#### NEW QUESTION 12

- (Exam Topic 1)

A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using AWS. The company's security team has enabled Amazon

GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining

How can the security team continue using GuardDuty while meeting these requirements?

- A. In the GuardDuty console, select the CryptoCurrency:EC2/BitcoinTool B'DNS finding and use the suppress findings option
- B. Create a custom AWS Lambda function to process newly detected GuardDuty alerts Process the CryptoCurrency EC2/BitcoinTool BIDNS alert and filter outthe high-severity finding types only.
- C. When creating a new Amazon EC2 Instance, provide the instance with a specific tag that indicates it is performing mining operations Create a custom AWS Lambda function to process newly detected GuardDuty alerts and filter for the presence of this tag
- D. When GuardDuty produces a cryptocurrency finding, process the finding with a custom AWS Lambda function to extract the instance ID from the finding Then use the AWS Systems Manager Run Command to check for a running process performing mining operations

**Answer:** A

#### NEW QUESTION 14

- (Exam Topic 1)

A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an AWS CloudFormation template. The Engineer notices instances terminating right after they are launched.

What could be causing these terminations?

- A. The IAM user launching those instances is missing ec2:Runinstances permission.
- B. The AMI used as encrypted and the IAM does not have the required AWS KMS permissions.
- C. The instance profile used with the EC2 instances in unable to query instance metadata.
- D. AWS currently does not have sufficient capacity in the Region.

**Answer:** C

#### NEW QUESTION 17

- (Exam Topic 1)

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? (Select 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 up-to-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 external-facing systems to allow AWS to actively block malicious network traffic affecting Amazon EC2 instances.

**Answer:** BD

#### NEW QUESTION 22

- (Exam Topic 1)

A company has decided to use encryption in its AWS account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16.000 B to 5 MB. The requirements are as follows:

- The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
  - The key material must be available in multiple Regions. Which option meets these requirements?
- A. Use an AWS KMS customer managed key and store the key material in AWS with replication across Regions
- B. Use an AWS customer managed key, import the key material into AWS KMS using in-house AWS CloudHS
- C. and store the key material securely in Amazon S3.
- D. Use an AWS KMS custom key store backed by AWS CloudHSM clusters, and copy backups across Regions
- E. Use AWS CloudHSM to generate the key material and backup keys across Regions Use the Java Cryptography Extension (JCE) and Public Key Cryptography Standards #11 (PKCS #11) encryption libraries to encrypt and decrypt the data.

**Answer:** D

#### NEW QUESTION 24

- (Exam Topic 1)

A company's Director of information Security wants a daily email report from AWS that contains recommendations for each company account to meet AWS Security best practices.

Which solution would meet these requirements?

- A. in every AWS account, configure AWS Lambda to query the AWS Support API for AWS Trusted Advisor security checks Send the results from Lambda to an Amazon SNS topic to send reports.
- B. Configure Amazon GuardDuty in a master account and invite all other accounts to be managed by the master account Use GuardDuty's integration with Amazon SNS to report on findings
- C. Use Amazon Athena and Amazon QuickSight to build reports off of AWS CloudTrail Create a daily Amazon CloudWatch trigger to run the report daily and email it using Amazon SNS
- D. Use AWS Artifact's prebuilt reports and subscriptions Subscribe the Director of Information Security to the reports by adding the Director as the security alternate contact for each account

**Answer:** A

#### NEW QUESTION 25

- (Exam Topic 1)

An application developer is using an AWS Lambda function that must use AWS KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB Which key policy would allow the application to do this while granting least privilege?

- A.
- ```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:*"
  ],
  "Resource": "*"
}
```
- B.
- ```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```
- C.
- ```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

D. 

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Disable*",
    "kms:Decrypt"
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

### NEW QUESTION 30

- (Exam Topic 1)

A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer. Assuming that AWS Certificate Manager is used, how many certificates will need to be generated?

- A. One in the US West (Oregon) region and one in the US East (Virginia) region.
- B. Two in the US West (Oregon) region and none in the US East (Virginia) region.
- C. One in the US West (Oregon) region and none in the US East (Virginia) region.
- D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

**Answer: B**

### NEW QUESTION 31

- (Exam Topic 1)

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region. What policy should the Engineer implement?

A 

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

B

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    }
  ]
}
```

C

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

D

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "NotAction": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

### NEW QUESTION 32

- (Exam Topic 1)

A company's data lake uses Amazon S3 and Amazon Athena. The company's security engineer has been asked to design an encryption solution that meets the company's data protection requirements. The encryption solution must work with Amazon S3 and keys managed by the company. The encryption solution must be protected in a hardware security module that is validated to Federal Information Processing Standards (FIPS) 140-2 Level 3.

Which solution meets these requirements?

- A. Use client-side encryption with an AWS KMS customer-managed key implemented with the AWS Encryption SDK
- B. Use AWS CloudHSM to store the keys and perform cryptographic operations. Save the encrypted text in Amazon S3
- C. Use an AWS KMS customer-managed key that is backed by a custom key store using AWS CloudHSM
- D. Use an AWS KMS customer-managed key with the bring your own key (BYOK) feature to import a key stored in AWS CloudHSM

**Answer: B**

### NEW QUESTION 33

- (Exam Topic 1)

A company is operating an open-source software platform that is internet-facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon Route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon RDS database. A recent report suggests this software platform is vulnerable to SQL injection attacks, with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The security engineer's solution involves the least amount of effort and maintains normal operations during implementation.

What should the security engineer do to meet these requirements?

- A. Create an Application Load Balancer with the existing EC2 instances as a target group. Create an AWS WAF web ACL containing rules that protect the application from this attack.
- B. Then apply it to the ALB. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the ALB. Update security groups on the EC2 instances to prevent direct access from the internet.
- C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the distribution. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront.
- D. Obtain the latest source code for the platform and make the necessary updates. Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances.
- E. Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances. Test to ensure the vulnerability has been mitigated.
- F. Then restore the security group to the original setting.

**Answer: A**

### NEW QUESTION 38

- (Exam Topic 1)

After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "10.10.10.0/24"
          ]
        }
      }
    }
  ]
}
```

Is this bucket policy sufficient to ensure that the data is not publicly accessible?

- A. Yes, the bucket policy makes the whole bucket publicly accessible despite how the S3 bucket ACL or object ACLs are configured.
- B. Yes, none of the data in the bucket is publicly accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
- C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.
- D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

**Answer: A**

### NEW QUESTION 43

- (Exam Topic 1)

A company plans to use custom AMIs to launch Amazon EC2 instances across multiple AWS accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed AWS KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups.

Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute tasks?

- A. Create a customer-managed CMK in the centralized account.
- B. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy. Create an IAM role in all applicable accounts and configure its access policy to allow the use of the centrally managed CMK for cryptographic operations.
- C. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.



- D. Create a customer-managed CMK in the centralized account
- E. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- F. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CM
- G. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographic operations and with the EC2 Auto Scaling service-linked role defined as the grantee principal.
- H. Create a customer-managed CMK or an AWS managed CMK in the centralized account
- I. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- J. Use the CMK administrator to create a CMK grant that includes permissions to perform cryptographic operations that define EC2 Auto Scaling service-linked roles from all other accounts as the grantee principal.
- K. Create a customer-managed CMK or an AWS managed CMK in the centralized account
- L. Allow other applicable accounts to use that key for cryptographic operations by applying proper cross-account permissions in the key policy
- M. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographic operations against the centrally managed CMK.

**Answer:** B

#### NEW QUESTION 45

- (Exam Topic 1)

The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an AWS KMS customer managed key (CMK). Which CMK-related issues could be responsible? (Choose two.)

- A. The CMK specified in the application does not exist.
- B. The CMK specified in the application is currently in use.
- C. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
- D. The CMK specified in the application is not enabled.
- E. The CMK specified in the application is using an alias.

**Answer:** AD

#### Explanation:

[https://docs.amazonaws.cn/en\\_us/kms/latest/developerguide/services-parameter-store.html](https://docs.amazonaws.cn/en_us/kms/latest/developerguide/services-parameter-store.html)

#### NEW QUESTION 49

- (Exam Topic 1)

A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in AWS Systems Manager Parameter Store. When the application tries to access the secure string key value, it fails. Which factors could be the cause of this failure? (Select TWO.)

- A. The EC2 instance role does not have decrypt permissions on the AWS Key Management Service (AWS KMS) key used to encrypt the secret
- B. The EC2 instance role does not have read permissions to read the parameters in Parameter Store
- C. Parameter Store does not have permission to use AWS Key Management Service (AWS KMS) to decrypt the parameter
- D. The EC2 instance role does not have encrypt permissions on the AWS Key Management Service (AWS KMS) key associated with the secret
- E. The EC2 instance does not have any tags associated.

**Answer:** CE

#### NEW QUESTION 50

- (Exam Topic 1)

The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet. What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

- A. Use AWS Certificate Manager to encrypt all traffic between the client and application servers.
- B. Review the application security groups to ensure that only the necessary ports are open.
- C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
- D. Use Amazon Inspector to periodically scan the backend instances.
- E. Use AWS Key Management Services to encrypt all the traffic between the client and application servers.

**Answer:** BD

#### NEW QUESTION 55

- (Exam Topic 1)

A security engineer is asked to update an AWS CloudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the security engineer receives the following error message: "There is a problem with the bucket policy." What will enable the security engineer to save the change?

- A. Create a new trail with the updated log file prefix, and then delete the original trail. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
- B. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform PutBucketPolicy, and then update the log file prefix in the CloudTrail console.
- C. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform PutBucketPolicy, and then update the log file prefix in the CloudTrail console.
- D. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
- E. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform GetBucketPolicy, and then update the log file prefix in the CloudTrail console.

**Answer:** B

#### NEW QUESTION 58

- (Exam Topic 1)

Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured AWS Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid. Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

- A. Configure the S3 bucket ACLs to allow AWS Config to record changes to the buckets.
- B. Configure policies attached to S3 buckets to allow AWS Config to record changes to the buckets.
- C. Attach the AmazonS3ReadOnlyAccess managed policy to the IAM user.
- D. Verify the security engineer's IAM user has an attached policy that allows all AWS Config actions.
- E. Assign the AWSConfigRole managed policy to the AWS Config role

**Answer:** BE

#### NEW QUESTION 62

- (Exam Topic 1)

A Security Engineer manages AWS Organizations for a company. The Engineer would like to restrict AWS usage to allow Amazon S3 only in one of the organizational units (OUs). The Engineer adds the following SCP to the OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsS3",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

The next day, API calls to AWS IAM appear in AWS CloudTrail logs in an account under that OU. How should the Security Engineer resolve this issue?

- A. Move the account to a new OU and deny IAM:\* permissions.
- B. Add a Deny policy for all non-S3 services at the account level.
- C. Change the policy to: {"Version": "2012-10-17", "Statement": [{"Sid": "AllowS3", "Effect": "Allow", "Action": "s3:\*", "Resource": "/\*/\*"}]}
- D. Detach the default FullAWSAccess SCP

**Answer:** C

#### NEW QUESTION 63

- (Exam Topic 1)

A company's security engineer is configuring Amazon S3 permissions to ban all current and future public buckets. However, the company hosts several websites directly off S3 buckets with public access enabled.

The engineer needs to block public S3 buckets without causing any outages on the existing websites. The engineer has set up an Amazon CloudFront distribution for each website. Which set of steps should the security engineer implement next?

- A. Configure an S3 bucket as the origin and origin access identity (OAI) for the CloudFront distribution. Switch the DNS records from websites to point to the CloudFront distribution. Enable block public access settings at the account level.
- B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution. Switch the DNS records for the websites to point to the CloudFront distribution. Then, for each S3 bucket, enable block public access settings.
- C. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution. Enable block public access settings at the account level.
- D. Configure an S3 bucket as the origin for the CloudFront distribution. Configure the S3 bucket policy to accept connections from the CloudFront points of presence only. Switch the DNS records for the websites to point to the CloudFront distribution. Enable block public access settings at the account level.

**Answer:** A

#### NEW QUESTION 65

- (Exam Topic 1)

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.

After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the AWS account was compromised and Amazon EBS snapshots were deleted.

All EBS snapshots are encrypted using an AWS KMS CMK. Which solution would solve this problem?

- A. Create a new Amazon S3 bucket. Use EBS lifecycle policies to move EBS snapshots to the new S3 bucket.
- B. Move snapshots to Amazon S3 Glacier using lifecycle policies, and apply Glacier Vault Lock policies to prevent deletion.
- C. Use AWS Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.
- D. Create a new AWS account with limited privilege.
- E. Allow the new account to access the AWS KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recurring basis.
- F. Use AWS Backup to copy EBS snapshots to Amazon S3.

**Answer:** A

#### NEW QUESTION 67

- (Exam Topic 1)

A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs).

Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

- A. Log on to each EC2 instance, check and export the different software versions installed, and verify this against a list of current CVEs.
- B. Install the Amazon Inspector agent on all development instances Build a custom rule package, and configure Inspector to perform a scan using this custom rule on all instances tagged as being in the development environment.
- C. Install the Amazon Inspector agent on all development instances Configure Inspector to perform a scan using the CVE rule package on all instances tagged as being in the development environment.
- D. Install the Amazon EC2 System Manager agent on all development instances Issue the Run command to EC2 System Manager to update all instances
- E. Use AWS Trusted Advisor to check that all EC2 instances have been patched to the most recent version of operating system and installed software.

**Answer:** CD

#### NEW QUESTION 68

- (Exam Topic 1)

A developer is creating an AWS Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an AWS KMS Customer Master Key (CMK) supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.

Which of the following are required for this configuration to work? (Select TWO.)

- A. The developer must configure Lambda access to the VPC using the --vpc-config parameter.
- B. The Lambda function execution role must have the kms:Decrypt- permission added in the AWS IAM policy.
- C. The KMS key policy must allow permissions for the developer to use the KMS key.
- D. The AWS IAM policy assigned to the developer must have the kms:GenerateDataKey permission added.
- E. The Lambda execution role must have the kms:Encrypt permission added in the AWS IAM policy.

**Answer:** BC

#### NEW QUESTION 70

- (Exam Topic 1)

A Security Engineer accidentally deleted the imported key material in an AWS KMS CMK. What should the Security Engineer do to restore the deleted key material?

- A. Create a new CM
- B. Download a new wrapping key and a new import token to import the original key material
- C. Create a new CMK Use the original wrapping key and import token to import the original key material.
- D. Download a new wrapping key and a new import token Import the original key material into the existing CMK.
- E. Use the original wrapping key and import token Import the original key material into the existing CMK

**Answer:** C

#### NEW QUESTION 72

- (Exam Topic 1)

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns

Which solution would have the MOST scalability and LOWEST latency?

- A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
- B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
- C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers
- D. Configure Amazon Route 53 to use multivalued answer routing to send traffic to the containers

**Answer:** A

#### NEW QUESTION 77

- (Exam Topic 1)

A company is designing the secure architecture (or a global latency-sensitive web application it plans to deploy to AWS. A Security Engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.

Which solution meets these requirements?

- A. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region
- B. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- C. Create an Amazon CloudFront distribution that uses the ALB as its origin
- D. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
- E. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region
- F. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- G. Create an Amazon CloudFront distribution that uses the ALB as its origin
- H. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
- I. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region
- J. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- K. Create appropriate AWS WAF ACLs and enable them on the ALB.
- L. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region
- M. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- N. Create appropriate AWS WAF ACLs and enable them on the ALB.

**Answer:** A

#### NEW QUESTION 78

- (Exam Topic 1)

A security engineer has noticed that VPC Flow Logs are getting a lot of REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The



security engineer is concerned that this EC2 instance may be compromised.

What immediate action should the security engineer take? What immediate action should the security engineer take?

- A. Remove the instance from the Auto Scaling group Close the security group ingress only from a single forensic IP address to perform an analysis.
- B. Remove the instance from the Auto Scaling group Change the network ACL rules to allow traffic only from a single forensic IP address to perform an analysis. Add a rule to deny all other traffic.
- C. Remove the instance from the Auto Scaling group Enable Amazon GuardDuty in that AWS account Install the Amazon Inspector agent on the suspicious EC2 instance to perform a scan.
- D. Take a snapshot of the suspicious EC2 instance
- E. Create a new EC2 instance from the snapshot in a closed security group with ingress only from a single forensic IP address to perform an analysis

**Answer: B**

#### NEW QUESTION 82

- (Exam Topic 1)

A Developer reported that AWS CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.

What should the Security Engineer do to meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to monitor the AWS CloudTrail configuration
- B. Send notifications using Amazon SNS.
- C. Create an Amazon CloudWatch Events rule to monitor Amazon GuardDuty findings
- D. Send email notifications using Amazon SNS.
- E. Update security contact details in AWS account settings for AWS Support to send alerts when suspicious activity is detected.
- F. Use Amazon Inspector to automatically detect security issues
- G. Send alerts using Amazon SNS.

**Answer: B**

#### NEW QUESTION 87

- (Exam Topic 1)

A company is developing a new mobile app for social media sharing. The company's development team has decided to use Amazon S3 to store media files generated by mobile app users. The company wants to allow users to control whether their own files are public, private, or shared with other users in their social network. What should the development team do to implement the type of access control with the LEAST administrative effort?

- A. Use individual ACLs on each S3 object.
- B. Use IAM groups for sharing files between application social network users
- C. Store each user's files in a separate S3 bucket and apply a bucket policy based on the user's sharing settings
- D. Generate presigned URLs for each file access

**Answer: A**

#### NEW QUESTION 89

- (Exam Topic 1)

A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.

Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption, and allow for immediate destruction of the data.

Which solution will meet these requirements?

- A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data
- B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to generate and store a data encryption key for each customer.
- C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys
- D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store. Use CloudHSM to generate and store a new CMK for each customer.

**Answer: A**

#### NEW QUESTION 93

- (Exam Topic 1)

A company's security team has defined a set of AWS Config rules that must be enforced globally in all AWS accounts the company owns. What should be done to provide a consolidated compliance overview for the security team?

- A. Use AWS Organizations to limit AWS Config rules to the appropriate Regions, and then consolidate the Amazon CloudWatch dashboard into one AWS account.
- B. Use AWS Config aggregation to consolidate the views into one AWS account, and provide role access to the security team.
- C. Consolidate AWS Config rule results with an AWS Lambda function and push data to Amazon S3
- D. Use Amazon SNS to consolidate and alert when some metrics are triggered.
- E. Use Amazon GuardDuty to load data results from the AWS Config rules compliance status, aggregate GuardDuty findings of all AWS accounts into one AWS account, and provide role access to the security team.

**Answer: B**

#### NEW QUESTION 97

- (Exam Topic 1)

A Security Engineer is troubleshooting a connectivity issue between a web server that is writing log files to the logging server in another VPC. The Engineer has confirmed that a peering relationship exists between the two VPCs. VPC flow logs show that requests sent from the web server are accepted by the logging server but the web server never receives a reply.



Which of the following actions could fix this issue?

- A. Add an inbound rule to the security group associated with the logging server that allows requests from the web server
- B. Add an outbound rule to the security group associated with the web server that allows requests to the logging server.
- C. Add a route to the route table associated with the subnet that hosts the logging server that targets the peering connection
- D. Add a route to the route table associated with the subnet that hosts the web server that targets the peering connection

**Answer:** C

#### NEW QUESTION 101

- (Exam Topic 1)

A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:

- HTTPS needs to be enforced for all data in transit with specific ciphers.
- The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

- A. Set up an S3 bucket policy with the awssecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher
- B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with AWS WAF to allow access from the CloudFront IP ranges.
- C. Set up an S3 bucket policy with the aws:securetransport ke
- D. Configure the CloudFront origin access identity (OAI) with the S3 bucke
- E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
- F. Modify the CloudFront distribution to use AWS WA
- G. Force HTTPS on the S3 bucket with specific ciphers in the bucket polic
- H. Configure an HTTPS listener only for the AL
- I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
- J. Modify the CloudFront distribution to use the ALB as the origi
- K. Enforce an HTTPS listener on the AL
- L. Create a path-based routing rule on the ALB with proxies that connect lo Amazon S3. Create a bucket policy to allow access from these proxies only.A company
- M. A security engineer has installed the Systems Manager Agent on all server
- N. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to the
- O. The security engineer needs to perform verification steps before Session Manager will work on the servers.Which combination of steps should the security engineer perform? (Select THREE.)
- P. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.
- Q. Enable the advanced-instances tier in Systems Manager.
- R. Create a managed-instance activation for the on-premises servers.
- S. Reconfigure the Systems Manager Agent with the activation code and ID.
- T. Assign an IAM role to all of the on-premises servers.
- . Initiate an inventory collection with Systems Manager on the on-premises servers

**Answer:** CEF

#### NEW QUESTION 106

- (Exam Topic 1)

A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes The software engineering team needs to make changes that will address the audit findings.

Which set of steps should the software engineering team take?

- A. Use an AWS Key Management Service (AWS KMS) CM
- B. Encrypt the data at rest.
- C. Use AWS Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.
- D. Use a DynamoDB encryption clien
- E. Use client-side encryption and sign the table items
- F. Use the AWS Encryption SD
- G. Use client-side encryption and sign the table items.

**Answer:** A

#### NEW QUESTION 109

- (Exam Topic 2)

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack? Please select:

- A. Change the Inbound Security Groups to deny access from the suspecting IP
- B. Change the Outbound Security Groups to deny access from the suspecting IP
- C. Change the Inbound NACL to deny access from the suspecting IP
- D. Change the Outbound NACL to deny access from the suspecting IP

**Answer:** C

#### Explanation:

Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.

Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the following

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

#### NEW QUESTION 112

- (Exam Topic 2)

Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account. Please select:

- A. Delete the AWS keys for the root account
- B. Create IAM Groups
- C. Create IAM Roles
- D. Restrict access using IAM policies

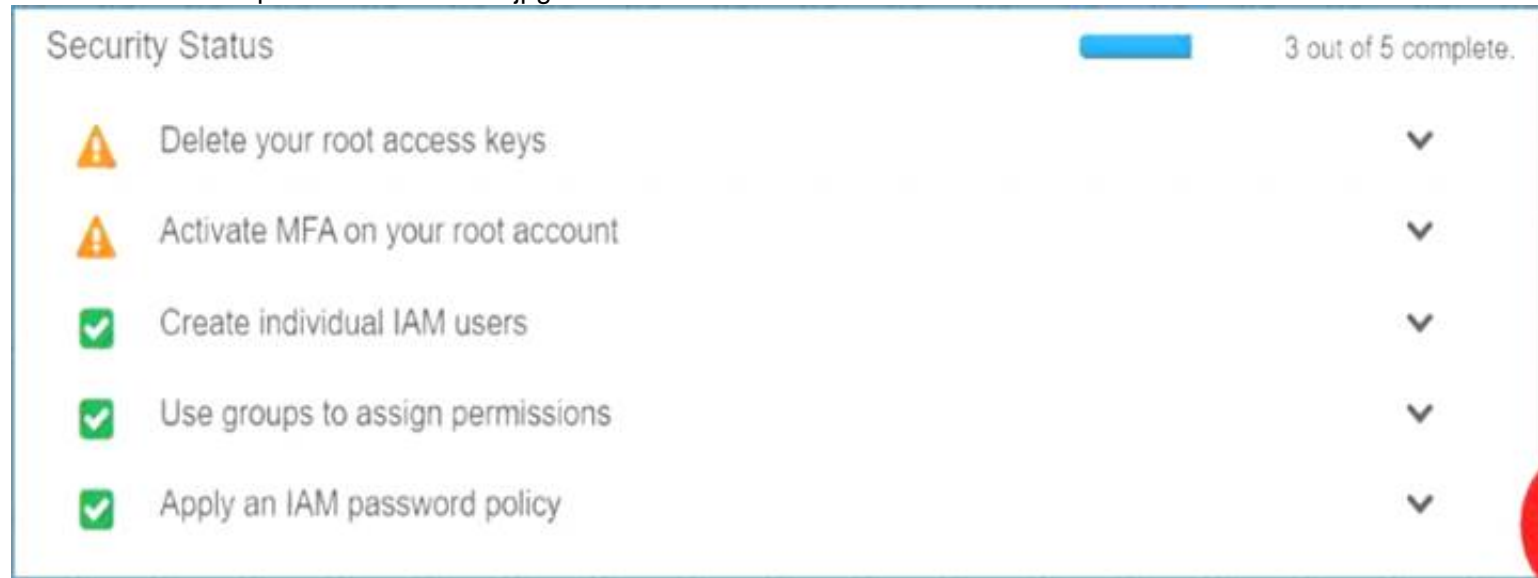
**Answer:** A

#### Explanation:

The first level or measure that should be taken is to delete the keys for the IAM root user

When you log into your account and go to your Security Access dashboard, this is the first step that can be seen

C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option B and C are wrong because creation of IAM groups and roles will not change the impact of leakage of AWS root access keys

Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL:

<https://docs.aws.amazon.com/eeneral/latest/gr/aws-access-keys-best-practices.html>

The correct answer is: Delete the AWS keys for the root account Submit your Feedback/Queries to our Experts

#### NEW QUESTION 117

- (Exam Topic 2)

You are devising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

```
{ "ID": "Policy1502987489630",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1502987487640",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::appbucket",
      "Principal": "*"
    }
  ]
}
```

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error Please select:

- A. Change the IAM permissions by applying PutBucketPolicy permissions.
- B. Verify that the policy has the same name as the bucket nam
- C. If no
- D. make it the same.
- E. Change the Resource section to "arn:aws:s3:::appbucket/\*".
- F. Create the bucket "appbucket" and then apply the policy.

**Answer:** C

**Explanation:**

When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the \* can be used to assign the permission to all objects in the bucket

Option A is invalid because the right permissions are already provided as per the question requirement Option B is invalid because it is not necessary that the policy has the same name as the bucket

Option D is invalid because this should be the default flow for applying the policy For more information on bucket policies please visit the below URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

The correct answer is: Change the Resource section to "arn:aws:s3:::appbucket/" Submit your Feedback/Queries to our Experts

**NEW QUESTION 118**

- (Exam Topic 2)

A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.

What combination of actions should the Engineer take? (Choose two.)

- A. Create an AWS Lambda function that determines whether Flow Logs are enabled for a given VPC.
- B. Create an AWS Config configuration item for each VPC in the company AWS account.
- C. Create an AWS Config managed rule with a resource type of AWS:: Lambda:: Function.
- D. Create an Amazon CloudWatch Event rule that triggers on events emitted by AWS Config.
- E. Create an AWS Config custom rule, and associate it with an AWS Lambda function that contains the evaluating logic.

**Answer:** AE

**Explanation:**

<https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-a>

**NEW QUESTION 122**

- (Exam Topic 2)

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted."

The security solution must meet all of the following requirements:

- Each object must be encrypted using a unique key.
- Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.
- AWS KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

- A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annuall
- B. For the "Restricted" CMK, define the MFA policy within the key polic
- C. Use S3 SSE-KMS to encrypt the objects.
- D. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to tru
- E. S3 can then use the grants to encrypt each object with a unique CMK.
- F. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA polic
- G. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
- H. Create a CMK with unique imported key material for each data classification type, and rotate them annuall
- I. For the "Restricted" key material, define the MFA policy in the key polic
- J. Use S3 SSE-KMS to encrypt the objects.

**Answer:** A

**Explanation:**

CMKs that are not eligible for automatic key rotation, including asymmetric CMKs, CMKs in custom key stores, and CMKs with imported key material.

**NEW QUESTION 126**

- (Exam Topic 2)

A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized AWS IAM user from the IP address range 10.10.10.0/24:

```
{
  "Version": "2012-10-17",
  "Id": "S3Policy1",
  "Statement": [
    {
      "Sid": ["OfficeAllowIP"],
      "Effect": ["Allow"],
      "Principal": ["*"],
      "Action": ["s3:*"],
      "Resource": ["arn:aws:s3:::Bucket"],
      "Condition": {
        "IpAddress": [
          {
            "aws: SourceIp": "10.10.10.0/24"
          }
        ]
      }
    }
  ]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message. What does the Administrator need to change to grant access to the user?

- A. Change the "Resource" from "arn: aws:s3:::Bucket" to "arn:aws:s3:::Bucket/\*".
- B. Change the "Principal" from "\*" to {AWS:"arn:aws:iam: : account-number: user/username"}
- C. Change the "Version" from "2012-10-17" to the last revised date of the policy
- D. Change the "Action" from ["s3:\*"] to ["s3:GetObject", "s3:ListBucket"]

**Answer:** A

#### NEW QUESTION 130

- (Exam Topic 2)

An AWS account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam: : 123456789012: user/alice"},
      "Action": "s3:*",
      "Resource": ["arn:aws:s3: : :bucket1", "arn:aws:s3: : :bucket1/*"]
    }
  ]
}
```

In addition, the same account has an IAM User named "alice", with the following IAM policy.



```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": ["arn:aws:s3:::bucket2", "arn:aws:s3:::bucket2/*"]
  }]
}
```

Which buckets can user "alice" access?

- A. Bucket1 only
- B. Bucket2 only
- C. Both bucket1 and bucket2
- D. Neither bucket1 nor bucket2

**Answer:** C

**Explanation:**

Both S3 policies and IAM policies can be used to grant access to buckets. IAM policies specify what actions are allowed or denied on what AWS resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance\_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or roles, which are then subject to the permissions you've defined. In other words, IAM policies define what a principal can do in your AWS environment. S3 bucket policies, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to (e.g. allow user Alice to PUT but not DELETE objects in the bucket).

<https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s>

**NEW QUESTION 132**

- (Exam Topic 2)

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.

**Answer:** B

**Explanation:**

[https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_data-sources.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html) [https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_backdoor.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_backdoor.html)

**NEW QUESTION 137**

- (Exam Topic 2)

A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.

Which approach will meet these requirements while protecting the external certificate during a breach?

- A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.
- B. Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instance
- C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
- D. Generate an internal self-signed certificate and apply it to the instance
- E. Use AWS Certificate Manager to generate a new external certificate for the EL
- F. Have the ELB decrypt traffic, and route and re-encrypt with the internal certificate.
- G. Upload a new external certificate to the load balance
- H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

**Answer:** C

**NEW QUESTION 141**

- (Exam Topic 2)

A company is using CloudTrail to log all AWS API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.

What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below  
Please select:

- A. Create an S3 bucket in a dedicated log account and grant the other accounts write only access
- B. Deliver all log files from every account to this S3 bucket.

- C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
- D. Run the function every 10 minutes.
- E. Enable CloudTrail log file integrity validation
- F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
- G. Create a Security Group that blocks all traffic except calls from the CloudTrail service
- H. Associate the security group with) all the Cloud Trail destination S3 buckets.

**Answer:** AC

**Explanation:**

The AWS Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.

Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-loc-file-validation-intro.html> For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.htm>

The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation

Submit your Feedback/Queries to our Experts

**NEW QUESTION 145**

- (Exam Topic 2)

What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Choose two.)

- A. Use the AWS account root user access keys instead of the AWS Management Console
- B. Enable multi-factor authentication for the AWS IAM users with the AdministratorAccess managed policy attached to them
- C. Enable multi-factor authentication for the AWS account root user
- D. Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days
- E. Do not create access keys for the AWS account root user; instead, create AWS IAM users

**Answer:** CE

**NEW QUESTION 148**

- (Exam Topic 2)

A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same AWS KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.

The company's Developer Operations department learns about this only after the CMK has been deleted. Which steps must be taken to address this situation?

- A. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
- B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.
- C. Make a request to AWS Support to recover the S3 encrypted data.
- D. Make a request to AWS Support to restore the deleted CMK, and use it to recover the data.

**Answer:** C

**NEW QUESTION 149**

- (Exam Topic 2)

The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault.

What is the MOST cost-effective way to correct this?

- A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
- B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
- C. Update the policy, keeping the vault lock in place.
- D. Update the policy and call initiate-vault-lock again to apply the new policy.

**Answer:** A

**Explanation:**

Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires. Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API. <https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html>

**NEW QUESTION 153**

- (Exam Topic 2)

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.

What techniques will limit lateral movement and allow evidence gathering?

- A. Remove the instance from the load balancer and terminate it.
- B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
- C. Reboot the instance and check for any Amazon CloudWatch alarms.
- D. Stop the instance and make a snapshot of the root EBS volume.

**Answer:** B

**Explanation:**

[https://d1.awsstatic.com/whitepapers/aws\\_security\\_incident\\_response.pdf](https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf)

**NEW QUESTION 155**

- (Exam Topic 2)

A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.

Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

- A. Have a Database Administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.
- B. Configure a scheduled job that updates the credential in AWS Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.
- C. Configure automatic rotation of credentials in AWS Secrets Manager.
- D. Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Store.
- E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.
- F. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotated.
- G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

**Answer:** CE

**NEW QUESTION 157**

- (Exam Topic 2)

A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report. How can the security team fulfill these requirements?

Please select:

- A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- B. Use Systems Manager Patch Manager to generate the report of out of compliance instances/ server.
- C. Use Systems Manager Patch Manager to install the missing patches.
- D. Use Systems Manager Patch Manager to generate the report of out of compliance instances/ servers. Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
- E. Use Trusted Advisor to generate the report of out of compliance instances/server.
- F. Use Systems Manager Patch Manager to install the missing patches.

**Answer:** B

**Explanation:**

Use the Systems Manager Patch Manager to generate the report and also install the missing patches. The AWS Documentation mentions the following: AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.

Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers.

Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.

For more information on the AWS Patch Manager, please visit the below URL:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html> (

The correct answer is: Use Systems Manager Patch Manager to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manager to install the missing patches.

Submit your Feedback/Queries to our Experts

**NEW QUESTION 161**

- (Exam Topic 2)

An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.

What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

- A. Configure and assign an MFA device to the role used by the instances.
- B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
- C. Verify that the access key attached to the role used by the instances is active.
- D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
- E. Verify that the role attached to the instances contains policies that allow access to the queue.

**Answer:** BE

**NEW QUESTION 165**

- (Exam Topic 2)

A company uses AWS Organization to manage 50 AWS accounts. The finance staff members log in as AWS IAM users in the FinanceDept AWS account. The staff members need to read the consolidated billing information in the MasterPayer AWS account. They should not be able to view any other resources in the MasterPayer AWS account. IAM access to billing has been enabled in the MasterPayer account.

Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?



- A. Create an IAM group for the finance users in the FinanceDept account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.
- B. Create an IAM group for the finance users in the MasterPayer account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.
- C. Create an AWS IAM role in the FinanceDept account with the ViewBilling permission, then grant the finance users in the MasterPayer account the permission to assume that role.
- D. Create an AWS IAM role in the MasterPayer account with the ViewBilling permission, then grant the finance users in the FinanceDept account the permission to assume that role.

**Answer:** D

**Explanation:**

AWS Region that You Request a Certificate In (for AWS Certificate Manager) If you want to require HTTPS between viewers and CloudFront, you must change the AWS region to US East (N. Virginia) in the AWS Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you're using an ELB load balancer as your origin, you can request or import a certificate in any region.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

**NEW QUESTION 167**

- (Exam Topic 2)

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:

Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an AWS account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

- A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.
- B. Block outbound access to public S3 endpoints on the proxy server.
- C. Configure Network ACLs on Server X to deny access to S3 endpoints.
- D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.
- E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

**Answer:** AB

**NEW QUESTION 169**

- (Exam Topic 2)

Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet.

Which of the following mitigations should be recommended?

- A. Use AWS Config to detect whether an Internet Gateway is added and use an AWS Lambda function to provide auto-remediation.
- B. Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.
- C. Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.
- D. Move the workload to a Dedicated Host, as this provides additional network security controls and monitoring.

**Answer:** A

**Explanation:**

By default, Private instance has a private IP address, but no public IP address. These instances can communicate with each other, but can't access the Internet. You can enable Internet access for an instance launched into a nondefault subnet by attaching an Internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance. Alternatively, to allow an instance in your VPC to initiate outbound connections to the Internet but prevent unsolicited inbound connections from the Internet, you can use a network address translation (NAT) instance. NAT maps multiple private IP addresses to a single public IP address. A NAT instance has an Elastic IP address and is connected to the Internet through an Internet gateway. You can connect an instance in a private subnet to the Internet through the NAT instance, which routes traffic from the instance to the Internet gateway, and routes any responses to the instance.

**NEW QUESTION 173**

- (Exam Topic 2)

A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment. What configuration is necessary to allow the virtual security appliance to route the traffic?

- A. Disable network ACLs.
- B. Configure the security appliance's elastic network interface for promiscuous mode.
- C. Disable the Network Source/Destination check on the security appliance's elastic network interface
- D. Place the security appliance in the public subnet with the internet gateway

**Answer:** C

**Explanation:**

Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. In this case virtual security appliance instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance."

**NEW QUESTION 177**

- (Exam Topic 2)

Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.

What steps are necessary to identify the cause of this phenomenon? (Choose two.)

- A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.



- B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
- C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
- D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
- E. Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

**Answer:** AB

**Explanation:**

[https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6\\_NybQPhh6tRP/Cloudwatch%](https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%20logs-agent-streaming)

**NEW QUESTION 178**

- (Exam Topic 2)

An application outputs logs to a text file. The logs must be continuously monitored for security incidents.

Which design will meet the requirements with MINIMUM effort?

- A. Create a scheduled process to copy the component's logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log data.
- B. Set up CloudWatch alerts based on the metrics.
- C. Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instance.
- D. Create a CloudWatch metric filter to monitor the application log.
- E. Set up CloudWatch alerts based on the metrics.
- F. Create a scheduled process to copy the application log files to AWS CloudTrail.
- G. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log data.
- H. Set up CloudWatch alerts based on the metrics.
- I. Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file. Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log data.
- J. Set up CloudWatch alerts based on the metrics.

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html>

**NEW QUESTION 182**

- (Exam Topic 2)

A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.

What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

- A. Store the scripts in the AMI and encrypt the sensitive data using AWS KMS. Use the instance role profile to control access to the KMS keys needed to decrypt the data.
- B. Store the sensitive data in AWS Systems Manager Parameter Store using the encrypted string parameter and assign the GetParameters permission to the EC2 instance role.
- C. Externalize the bootstrap scripts in Amazon S3 and encrypt them using AWS KMS.
- D. Remove the scripts from the instance and clear the logs after the instance is configured.
- E. Block user access of the EC2 instance's metadata service using IAM policies.
- F. Remove all scripts and clear the logs after execution.

**Answer:** B

**NEW QUESTION 184**

- (Exam Topic 2)

You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?

Please select:

- A. Enable AWS Guard Duty for the Instance
- B. Use AWS Trusted Advisor
- C. Use AWS Inspector
- D. Use AWS Macie

**Answer:** C

**Explanation:**

The AWS Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security.

Center for Internet security (CIS) Benchmarks

The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed here.

Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities. Options B and D are invalid because these services cannot give a list of vulnerabilities. For more information,

on the guidelines, please visit the below URL:

\* [https://docs.aws.amazon.com/inspector/latest/userguide/inspector\\_cis.html](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html) The correct answer is: Use AWS Inspector

Submit your Feedback/Queries to our Experts

**NEW QUESTION 186**

- (Exam Topic 2)

A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.

How can this be accomplished? (Choose two.)



- A. Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPC
- B. Do not complete the penetration test request form.
- C. Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VP
- D. Do not complete the penetration test request form.
- E. Create a VPN connection from the data center to VPC
- F. Use an on-premises scanning engine to scan the instances in all three VPC
- G. Complete the penetration test request form for all three VPCs.
- H. Create a VPN connection from the data center to each of the three VPC
- I. Use an on-premises scanning engine to scan the instances in each VP
- J. Do not complete the penetration test request form.
- K. Create a VPN connection from the data center to each of the three VPC
- L. Use an on-premises scanning engine to scan the instances in each VP
- M. Complete the penetration test request form for all three VPCs.

**Answer:** BD

**Explanation:**

<https://aws.amazon.com/security/penetration-testing/>

**NEW QUESTION 191**

- (Exam Topic 2)

You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

- A. C:\Users\wk\Desktop\mudassar\Untitled.jpg
 

```

"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent": true}
  }
}
      
```
- B. C:\Users\wk\Desktop\mudassar\Untitled.jpg
 

```

"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent":false}
  }
}
      
```
- C. C:\Users\wk\Desktop\mudassar\Untitled.jpg

```

    "Version": "2012-10-17",
    "Statement": {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": "Resource": "arn:aws:s3:::*",
      "Condition": {
        "aws:MultiFactorAuthPresent": false
      }
    }
  }
}

```

D. C:\Users\wk\Desktop\mudassar\Untitled.jpg "Version": "2012-10-17",

```

    "Statement": {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": "Resource": "arn:aws:s3:::*",
      "Condition": {
        "aws:MultiFactorAuthPresent": true
      }
    }
  }
}

```

**Answer:** A

#### Explanation:

The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the aws:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.

Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."

Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.

For more information on an example on such a policy, please visit the following URL:

#### NEW QUESTION 193

- (Exam Topic 2)

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.

Please select:

- A. Use the AWS Trusted Advisor to see what can be done.
- B. Use VPC Flow logs to diagnose the traffic
- C. Use AWS WAF to analyze the traffic
- D. Use AWS Guard Duty to analyze the traffic

**Answer:** B

#### Explanation:

Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application

Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application

Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application

The AWS Documentation mentions the following

VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security toi to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.

For more information on AWS Security, please visit the following URL: <https://aws.amazon.com/answers/networking/vpc-security-capabilities>>

The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

#### NEW QUESTION 198

- (Exam Topic 2)

A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:

- Users may access the website by using an Amazon CloudFront distribution.
- Users may not access the website directly by using an Amazon S3 URL.

Which configurations will support these requirements? (Choose two.)

- A. Associate an origin access identity with the CloudFront distribution.
- B. Implement a "Principal": "cloudfront.amazonaws.com" condition in the S3 bucket policy.
- C. Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.
- D. Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.
- E. Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

**Answer:** AC

#### NEW QUESTION 202

- (Exam Topic 2)

Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

- A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.
- B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
- C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
- D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

**Answer:** B

#### Explanation:

"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key."

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

#### NEW QUESTION 207

- (Exam Topic 2)

A corporate cloud security policy states that communications between the company's VPC and KMS must travel entirely within the AWS network and not use public service endpoints.

Which combination of the following actions MOST satisfies this requirement? (Choose two.)

- A. Add the aws:sourceVpce condition to the AWS KMS key policy referencing the company's VPC endpoint ID.
- B. Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.
- C. Create a VPC endpoint for AWS KMS with private DNS enabled.
- D. Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.
- E. Add the following condition to the AWS KMS key policy: "aws:SourceIp": "10.0.0.0/16".

**Answer:** AC

#### Explanation:

An IAM policy can deny access to KMS except through your VPC endpoint with the following condition statement:

```
"Condition": { "StringNotEquals": {  
  "aws:sourceVpce": "vpce-0295a3caf8414c94a"  
}
```

```
}
```

If you select the Enable Private DNS Name option, the standard AWS KMS DNS hostname (<https://kms.<region>.amazonaws.com>) resolves to your VPC endpoint.

#### NEW QUESTION 210

- (Exam Topic 2)

A company requires that IP packet data be inspected for invalid or malicious content. Which of the following approaches achieve this requirement? (Choose two.)

- A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through i
- B. Perform inspection within proxy software on the EC2 instance.
- C. Configure the host-based agent on each EC2 instance within the VP
- D. Perform inspection within the host-based agent.
- E. Enable VPC Flow Logs for all subnets in the VP
- F. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.
- G. Configure Elastic Load Balancing (ELB) access log
- H. Perform inspection from the log data within the ELB access log files.
- I. Configure the CloudWatch Logs agent on each EC2 instance within the VP
- J. Perform inspection from the log data within CloudWatch Logs.

**Answer:** AB

#### Explanation:

"EC2 Instance IDS/IPS solutions offer key features to help protect your EC2 instances. This includes alerting administrators of malicious activity and policy violations, as well as identifying and taking action against attacks. You can use AWS services and third party IDS/IPS solutions offered in AWS Marketplace to stay one step ahead of potential attackers."



#### NEW QUESTION 213

- (Exam Topic 2)

A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.

What would be the BEST way to reduce the potential impact of these attacks in the future?

- A. Use custom route tables to prevent malicious traffic from routing to the instances.
- B. Update security groups to deny traffic from the originating source IP addresses.
- C. Use network ACLs.
- D. Install intrusion prevention software (IPS) on each instance.

**Answer: D**

#### Explanation:

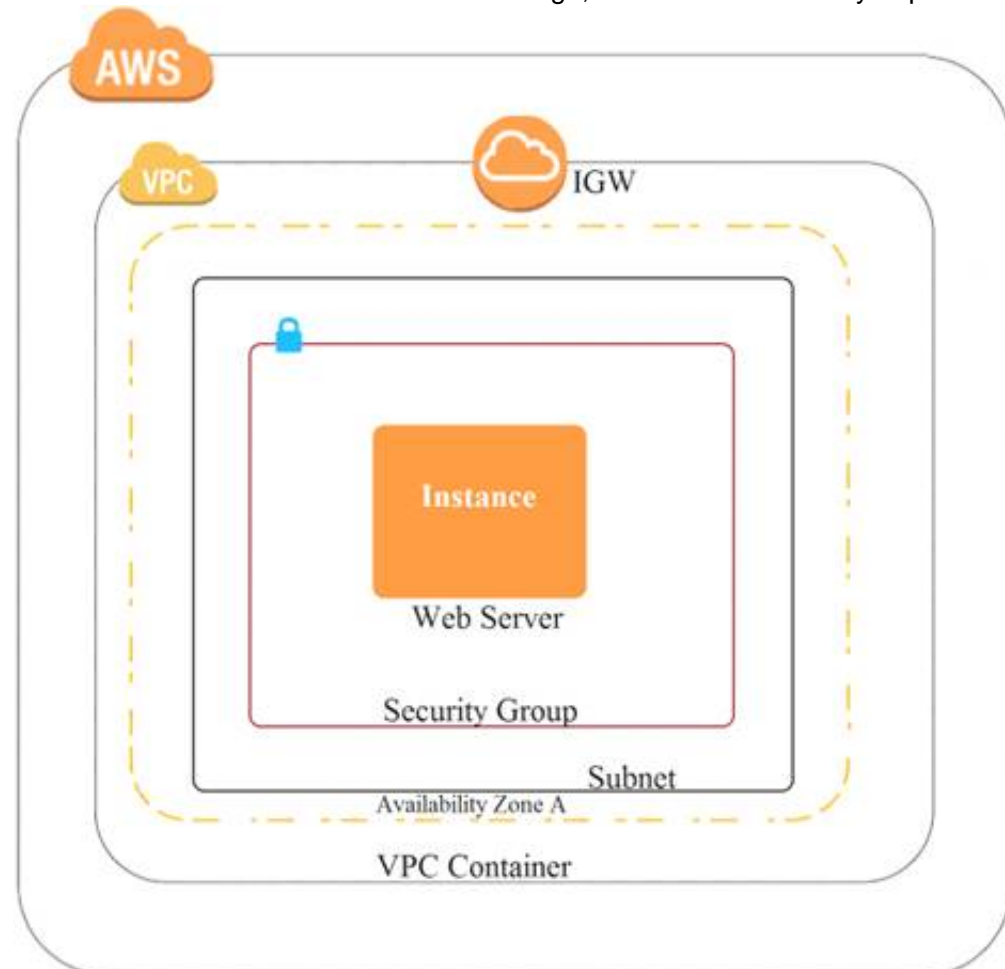
<https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html> NACL has limit 20 (can increase to maximum 40 rule), and more rule will make more low-latency

#### NEW QUESTION 214

- (Exam Topic 2)

A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.

Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?



- A. Move all the files to an Amazon S3 bucket
- B. Have the web server serve the files from the S3 bucket.
- C. Launch a second Amazon EC2 instance in a new subne
- D. Launch an Application Load Balancer in front of both instances.
- E. Launch an Application Load Balancer in front of the EC2 instanc
- F. Create an Amazon CloudFront distribution in front of the Application Load Balancer.
- G. Move all the files to an Amazon S3 bucke
- H. Create a CloudFront distribution in front of the bucket and terminate the web server.

**Answer: D**

#### Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

#### NEW QUESTION 217

- (Exam Topic 2)

A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:

- Content Security-Policy
- X-Frame-Options
- X-XSS-Protection

The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

- A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.
- B. Implement an AWS Lambda@Edge origin response function that inserts the required headers.
- C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.
- D. Construct an AWS WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

**Answer: B**

#### NEW QUESTION 221

- (Exam Topic 2)

A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old. Which of the following options should the Security Engineer use?

- A. In the AWS Console, choose the IAM service and select "Users". Review the "Access Key Age" column.
- B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
- C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
- D. Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.

**Answer: C**

#### Explanation:

[https://docs.aws.amazon.com/IAM/latest/APIReference/API\\_UpdateAccessKey.html](https://docs.aws.amazon.com/IAM/latest/APIReference/API_UpdateAccessKey.html)  
[https://docs.aws.amazon.com/IAM/latest/APIReference/API\\_GenerateCredentialReport.html](https://docs.aws.amazon.com/IAM/latest/APIReference/API_GenerateCredentialReport.html)  
[https://docs.aws.amazon.com/IAM/latest/APIReference/API\\_GetCredentialReport.html](https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetCredentialReport.html)

#### NEW QUESTION 222

- (Exam Topic 2)

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.

**Answer: BDE**

#### NEW QUESTION 226

- (Exam Topic 2)

An organization is moving non-business-critical applications to AWS while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in AWS. The internet performance is unpredictable. Which configuration will ensure continued connectivity between sites MOST securely?

- A. VPN and a cached storage gateway
- B. AWS Snowball Edge
- C. VPN Gateway over AWS Direct Connect
- D. AWS Direct Connect

**Answer: C**

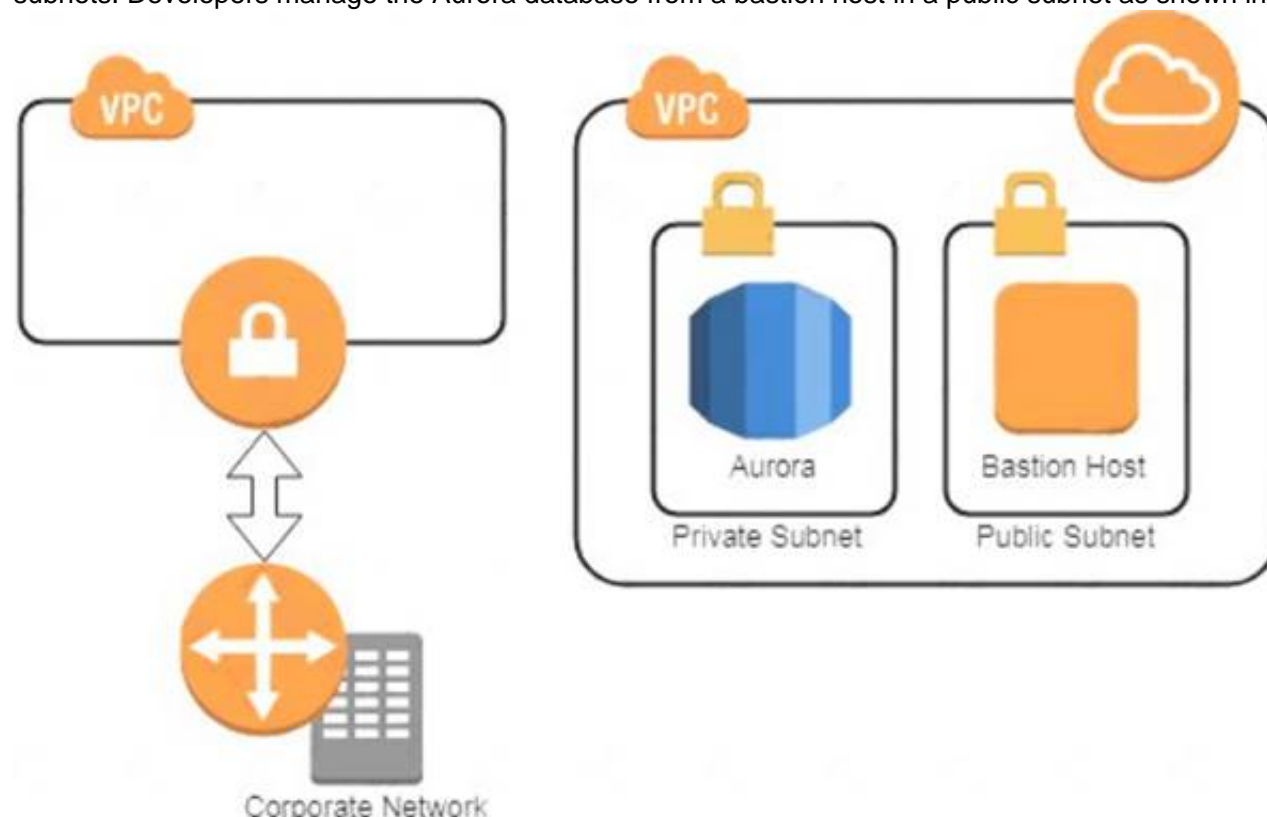
#### Explanation:

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-net>

#### NEW QUESTION 229

- (Exam Topic 2)

A company has two AWS accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.

How can a Security Engineer securely set up the bastion host?

- A. Move the bastion host to the VPC with VPN connectivity
- B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
- C. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
- D. Move the bastion host to the VPC with VPN connectivity
- E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
- F. Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

**Answer:** A

#### NEW QUESTION 231

- (Exam Topic 2)

An organization has a system in AWS that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes. A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks. Which solution would remediate the audit finding while minimizing the effort required?

- A. Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.
- B. Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.
- C. Use AWS Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service's servers.
- D. Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

**Answer:** C

#### NEW QUESTION 234

- (Exam Topic 2)

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability. Which of the following solutions will meet these requirements?

- A. Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.
- B. Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.
- C. Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.
- D. Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

**Answer:** B

#### Explanation:

<https://aws.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-usin>

#### NEW QUESTION 236

- (Exam Topic 2)

A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions. A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/JobFunctionRole"
      ],
      "Effect": "Allow"
    }
  ]
}
```

What should be done to enable the user to assume the appropriate role in the target account?

A Update the IAM policy attached to the role in the identity account to be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::123456789123:role/JobFunctionRole"
      ],
      "Effect": "Allow"
    }
  ]
}
```

B Update the trust policy on the role in the target account to be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::987654321987:role/IdentityRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

C Update the trust policy on the role in the identity account to be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::987654321987:root" },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

D Update the IAM policy attached to the role in the target account to be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1502946463000",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::123456789123:role/JobFunctionRole"
    }
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 239  
 - (Exam Topic 2)



A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by AWS Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days. After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

- A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.
- B. Enabling rotation in Secrets Manager causes the secret to rotate immediately, and the applications are using the earlier credential.
- C. The Secrets Manager IAM policy does not allow access to the RDS database.
- D. The Secrets Manager IAM policy does not allow access for the applications.

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/enable-rotation-rds.html>

**NEW QUESTION 240**

- (Exam Topic 2)

A company wants to control access to its AWS resources by using identities and groups that are defined in its existing Microsoft Active Directory. What must the company create in its AWS account to map permissions for AWS services to Active Directory user attributes?

- A. AWS IAM groups
- B. AWS IAM users
- C. AWS IAM roles
- D. AWS IAM access keys

**Answer:** C

**Explanation:**

Prerequisites to establish Federation Services in AWS - You have a working AD directory and AD FS server. - You have created an identity provider (IdP) in your AWS account using your XML file from your AD FS server. Remember the name of your IdP because you will use it later in this solution. -You have created the appropriate IAM roles in your AWS account, which will be used for federated access. <https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-activ>

**NEW QUESTION 243**

- (Exam Topic 2)

The Security team believes that a former employee may have gained unauthorized access to AWS resources sometime in the past 3 months by using an identified access key.

What approach would enable the Security team to find out what the former employee may have done within AWS?

- A. Use the AWS CloudTrail console to search for user activity.
- B. Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.
- C. Use AWS Config to see what actions were taken by the user.
- D. Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

**Answer:** A

**Explanation:**

You can use CloudTrail to search event history for the last 90 days. You can use CloudWatch queries to search API history beyond the last 90 days. You can use Athena to query CloudTrail logs over the last 90 days. <https://aws.amazon.com/premiumsupport/knowledge-center/view-iam-history/>

**NEW QUESTION 248**

- (Exam Topic 2)

Which of the following minimizes the potential attack surface for applications?

- A. Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
- B. Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific AWS resource.
- C. Use AWS Direct Connect for secure trusted connections between EC2 instances within private subnets.
- D. Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/answers/networking/vpc-security-capabilities/> Security Group is stateful and hypervisor level.

**NEW QUESTION 250**

- (Exam Topic 2)

An Amazon S3 bucket is encrypted using an AWS KMS CMK. An IAM user is unable to download objects from the S3 bucket using the AWS Management Console; however, other users can download objects from the S3 bucket.

Which policies should the Security Engineer review and modify to resolve this issue? (Select three.)

- A. The CMK policy
- B. The VPC endpoint policy
- C. The S3 bucket policy
- D. The S3 ACL
- E. The IAM policy

**Answer:** CDE

#### NEW QUESTION 254

- (Exam Topic 2)

You have an EC2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective  
Please select:

- A. Use a VPC endpoint
- B. Attach an Internet gateway to the subnet
- C. Attach a VPN connection to the VPC
- D. Use VPC Peering

**Answer:** A

#### Explanation:

The AWS Documentation mentions the following

You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and AWS KMS is conducted entirely within the AWS network.

Option B is invalid because this could open threats from the internet

Option C is invalid because this is normally used for communication between on-premise environments and AWS.

Option D is invalid because this is normally used for communication between VPCs

For more information on accessing KMS via an endpoint, please visit the following URL <https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html>

The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

#### NEW QUESTION 257

- (Exam Topic 2)

Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

- A. IAM User name and password
- B. Key pairs
- C. AWS Access keys
- D. AWS SDK keys

**Answer:** B

#### Explanation:

The AWS Documentation mentions the following

Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.

Option A, C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on AWS Security credentials, please visit the below URL: <https://docs.aws.amazon.com/eeneral/latest/er/aws-sec-cred-types.html>

The correct answer is: Key pairs

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 258

- (Exam Topic 2)

The Security Engineer for a mobile game has to implement a method to authenticate users so that they can save their progress. Because most of the users are part of the same OpenID-Connect compatible social media website, the Security Engineer would like to use that as the identity provider.

Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

- A. Amazon Cognito
- B. AssumeRoleWithWebIdentity API
- C. Amazon Cloud Directory
- D. Active Directory (AD) Connector

**Answer:** A

#### NEW QUESTION 260

- (Exam Topic 2)

A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification.

What is the MOST efficient way to meet these requirements?

- A. Install antivirus software and ensure that signatures are up-to-date
- B. Configure Amazon CloudWatch alarms to send alerts for security events.
- C. Install host-based IDS software to check for file integrity
- D. Export the logs to Amazon CloudWatch Logs for monitoring and alerting.
- E. Export system log files to Amazon S3. Parse the log files using an AWS Lambda function that will send alerts of any unauthorized system login attempts through Amazon SNS.
- F. Use Amazon CloudWatch Logs to detect file system change
- G. If a change is detected, automatically terminate and recreate the instance from the most recent AMI
- H. Use Amazon SNS to send notification of the event.

**Answer:** B

#### NEW QUESTION 263

- (Exam Topic 2)

An organization has tens of applications deployed on thousands of Amazon EC2 instances. During testing, the Application team needs information to let them know whether the network access control lists (network ACLs) and security groups are working as expected.

How can the Application team's requirements be met?

- A. Turn on VPC Flow Logs, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- B. Install an Amazon Inspector agent on each EC2 instance, send the logs to Amazon S3, and use Amazon EMR to query the logs.
- C. Create an AWS Config rule for each network ACL and security group configuration, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- D. Turn on AWS CloudTrail, send the trails to Amazon S3, and use AWS Lambda to query the trails.

**Answer:** A

#### NEW QUESTION 265

- (Exam Topic 2)

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.

**Answer:** B

#### NEW QUESTION 270

- (Exam Topic 2)

A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in AWS CloudTrail to support and troubleshoot the product.

Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

- A. Ensure that the log file integrity validation mechanism is enabled.
- B. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
- C. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
- D. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing—but not modifying—the log files.
- E. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.

**Answer:** AD

#### NEW QUESTION 273

- (Exam Topic 3)

You have a set of application, database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?

Please select:

- A. Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group
- B. Check the Outbound security rules for the database security group I Check the inbound security rules for the application security group
- C. Check the both the Inbound and Outbound security rules for the database security group Check the inbound security rules for the application security group
- D. Check the Outbound security rules for the database security group Check the both the Inbound and Outbound security rules for the application security group

**Answer:** A

#### Explanation:

Here since the communication would be established inward to the database server and outward from the application server, you need to ensure that just the Outbound rules for application server security groups are checked. And then just the Inbound rules for database server security groups are checked.

Option B can't be the correct answer. It says that we need to check the outbound security group which is not needed.

We need to check the inbound for DB SG and outbound of Application SG. Because, this two group need to communicate with each other to function properly.

Option C is invalid because you don't need to check for Outbound security rules for the database security group

Option D is invalid because you don't need to check for Inbound security rules for the application security group

For more information on Security Groups, please refer to below URL:

The correct answer is: Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 276

- (Exam Topic 3)

Your company has a hybrid environment, with on-premise servers and servers hosted in the AWS cloud. They are planning to use the Systems Manager for patching servers. Which of the following is a pre-requisite for this to work?

Please select:

- A. Ensure that the on-premise servers are running on Hyper-V.
- B. Ensure that an IAM service role is created
- C. Ensure that an IAM User is created
- D. Ensure that an IAM Group is created for the on-premise servers

**Answer:** B

#### Explanation:

You need to ensure that an IAM service role is created for allowing the on-premise servers to communicate with the AWS Systems Manager.

Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that IAM users

and groups are created For more information on the Systems Manager role please refer to the below URL: [com/systems-rnanaeer/latest/useruide/sysman-!](https://com/systems-rnanaeer/latest/useruide/sysman-!)  
 The correct answer is: Ensure that an IAM service role is created Submit your Feedback/Queries to our Experts

#### NEW QUESTION 279

- (Exam Topic 3)

A company created an AWS account for its developers to use for testing and learning purposes Because MM account will be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.

Developers were Instructed to tag al their instances with a Team tag key and use the team name in the tag value One of the first teams to use this account is

Business Intelligence A security engineer needs to develop a

highly scalable solution for providing developers with access to the appropriate resources within the account The security engineer has already created individual 1AM roles for each team.

Which additional configuration steps should the security engineer take to complete the task?

A. For each team, create an AM policy similar to the one that fellows Populate the ec2: ResourceTag/Team condition key with a proper team name Attach resulting policies to the corresponding 1AM roles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Team": "BusinessIntelligence"
        }
      }
    }
  ]
}
```

B. For each team create an 1AM policy similar to the one that follows Populate the aws TagKeys/Team condition key with a proper team nam

C. Attach the resuming policies to the corresponding 1AM roles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys/Team": "BusinessIntelligence"
        }
      }
    }
  ]
}
```

D. Tag each 1AM role with a Team lag ke

E. and use the team name in the tag valu

F. Create an 1AM policy similar to the one that follows, and attach 4 to all the 1AM roles used by developers.



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Team": "${aws:PrincipalTag/Team}"
        }
      }
    }
  ]
}
```

G. Tag each IAM role with the Team key, and use the team name in the tag value

H. Create an IAM policy similar to the one that follows, and attach it to all the IAM roles used by developers.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys/Team": "${aws:PrincipalTag/Team}"
        }
      }
    }
  ]
}
```

**Answer:** A

### NEW QUESTION 283

- (Exam Topic 3)

A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.

Please select:

- A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation
- B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
- C. Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
- D. Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

**Answer:** C

#### Explanation:

Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.

The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.

Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originates from the IT admin's workstation.

The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

### NEW QUESTION 288

- (Exam Topic 3)

You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script from S3 that deploys an application via GIT.

Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.

Please select:

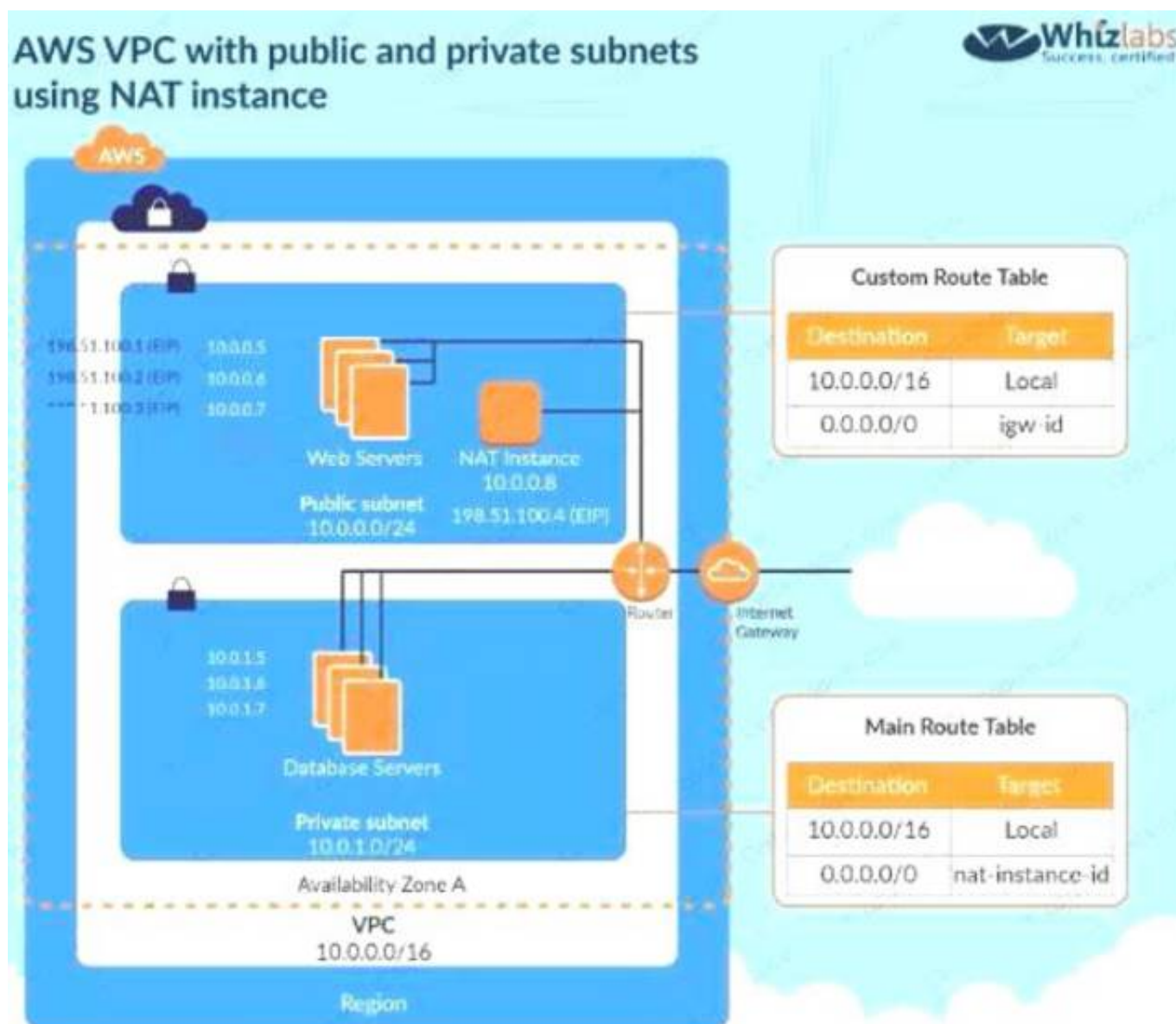
- A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
- B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
- C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
- D. EC2 instances in our private subnet, no EIPs, route outgoing traffic via the NAT

**Answer:** D

#### Explanation:

The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.

C:\Users\wk\Desktop\mudassar\Untitled.jpg



Options A and B are invalid because the instances need to be in the private subnet

Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance

For more information on NAT instance, please refer to the below Link: <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC Instance.html>!

The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

#### NEW QUESTION 291

- (Exam Topic 3)

An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below

Please select:

- A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag
- B. <
- C. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance call.
- D. Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
- E. Modify the IAM policy on the user to require MFA before deleting EC2 instances

**Answer:** AB

#### Explanation:

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define

Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL: [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins_Tags.html)

The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 296

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C01 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C01 Product From:

<https://www.2passeasy.com/dumps/SCS-C01/>

## Money Back Guarantee

### SCS-C01 Practice Exam Features:

- \* SCS-C01 Questions and Answers Updated Frequently
- \* SCS-C01 Practice Questions Verified by Expert Senior Certified Staff
- \* SCS-C01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SCS-C01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year