

# Amazon-Web-Services

## Exam Questions SCS-C01

AWS Certified Security- Specialty



### 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 has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.

The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a requirement that traffic between the web servers and the internet flow through the virtual security appliance.

The Security Engineer has verified the following:

- \* 1. The rule set in the Security Groups is correct
- \* 2. The rule set in the network ACLs is correct
- \* 3. The rule set in the virtual appliance is correct

Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)

- A. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.
- B. Verify which Security Group is applied to the particular web server's elastic network interface (ENI).
- C. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.
- D. Verify the registered targets in the ALB.
- E. Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

**Answer: CD**

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>

### NEW QUESTION 3

- (Exam Topic 1)

A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on AWS, but does have AWS Systems Manager configured. The solution must also minimize administrative overhead.

What should a security engineer recommend to meet these requirements?

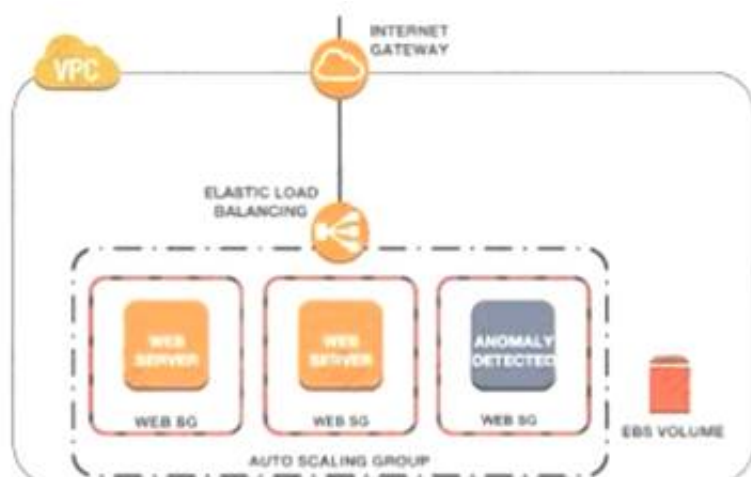
- A. Create an AWS Config rule defining the patch as a required configuration for EC2 instances.
- B. Use the AWS Systems Manager Run Command to patch affected instances.
- C. Use an AWS Systems Manager Patch Manager predefined baseline to patch affected instances.
- D. Use AWS Systems Manager Session Manager to log in to each affected instance and apply the patch.

**Answer: B**

### NEW QUESTION 4

- (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 is causing the anomaly. What are the MOST effective steps to take to 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 EBS 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 5

- (Exam Topic 1)

A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances wilt be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:

- Set up the proxy software on the EC2 instances.
- Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
- Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.

However, the proxy EC2 instances are not successfully forwarding traffic to the internet.

What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

- A. Put all the proxy EC2 instances in a cluster placement group.
- B. Disable source and destination checks on the proxy EC2 instances.
- C. Open all inbound ports on the proxy EC2 instance security group.
- D. Change the VPC's DHCP domain-name-servers options set to the IP addresses of proxy EC2 instances.

**Answer: B**

#### NEW QUESTION 6

- (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 7

- (Exam Topic 1)

A company uses HTTP Live Streaming (HLS) to stream live video content to paying subscribers by using Amazon CloudFront. HLS splits the video content into chunks so that the user can request the right chunk based on different conditions Because the video events last for several hours, the total video is made up of thousands of chunks

The origin URL is not disclosed and every user is forced to access the CloudFront URL The company has a web application that authenticates the paying users against an internal repository and a CloudFront key pair that is already issued.

What is the simplest and MOST effective way to protect the content?

- A. Develop the application to use the CloudFront key pair to create signed URLs that users will use to access the content.
- B. Develop the application to use the CloudFront key pair to set the signed cookies that users will use to access the content.
- C. Develop the application to issue a security token that Lambda@Edge will receive to authenticate and authorize access to the content
- D. Keep the CloudFront URL encrypted inside the application, and use AWS KMS to resolve the URL on-the-fly after the user is authenticated.

**Answer: B**

#### NEW QUESTION 8

- (Exam Topic 1)

A Security Engineer is setting up an AWS CloudTrail trail for all regions in an AWS account. For added security, the logs are stored using server-side encryption with AWS KMS-managed keys (SSE-KMS) and have log integrity validation enabled.

While testing the solution, the Security Engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

- A. The log files fail integrity validation and automatically are marked as unavailable.
- B. The KMS key policy does not grant the Security Engineer's IAM user or role permissions to decrypt with it.
- C. The bucket is set up to use server-side encryption with Amazon S3-managed keys (SSE-S3) as the default and does not allow SSE-KMS-encrypted files.
- D. An IAM policy applicable to the Security Engineer's IAM user or role denies access to the "CloudTrail/" prefix in the Amazon S3 bucket

**Answer: D**

#### NEW QUESTION 9

- (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 10

- (Exam Topic 1)

A company requires that SSH commands used to access its AWS instance be traceable to the user who executed each command. How should a Security Engineer accomplish this?

- A. Allow inbound access on port 22 at the security group attached to the instance Use AWS Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch logging for Systems Manager sessions
- B. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each user Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance
- C. Deny inbound access on port 22 at the security group attached to the instance Use AWS Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch logging for Systems Manager sessions
- D. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each team or group Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 1)

A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext. Which action would provide the required functionality?

- A. Pass the key alias to AWS KMS when calling Encrypt and Decrypt API actions.
- B. Use IAM policies to restrict access to Encrypt and Decrypt API actions.
- C. Use kms:EncryptionContext as a condition when defining IAM policies for the CMK.
- D. Use key policies to restrict access to the appropriate IAM groups.

**Answer:** B

#### NEW QUESTION 14

- (Exam Topic 1)

A company's on-premises data center forwards DNS logs to a third-party security incident events management (SIEM) solution that alerts on suspicious behavior. The company wants to introduce a similar capability to its AWS accounts that includes automatic remediation. The company expects to double in size within the next few months. Which solution meets the company's current and future logging requirements?

- A. Enable Amazon GuardDuty and AWS Security Hub in all Regions and all account
- B. Designate a master security account to receive all alerts from the child account
- C. Set up specific rules within Amazon EventBridge to trigger an AWS Lambda function for remediation steps.
- D. Ingest all AWS CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security account
- E. Use the current on-premises SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
- F. Ingest all AWS CloudTrail logs, VPC Flow Logs, and DNS logs into a single Amazon S3 bucket in a designated security account
- G. Launch an Amazon EC2 instance and install the current SIEM to monitor the logs and send a notification to an Amazon SNS topic to alert the security team of remediation steps.
- H. Enable Amazon GuardDuty and AWS Security Hub in all Regions and all account
- I. Designate a master security account to receive all alerts from the child account
- J. Create an AWS Organizations SCP that denies access to certain API calls that are on an ignore list.

**Answer:** A

#### NEW QUESTION 15

- (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 20

- (Exam Topic 1)

An organization policy states that all encryption keys must be automatically rotated every 12 months. Which AWS Key Management Service (KMS) key type should be used to meet this requirement?

- A. AWS managed Customer Master Key (CMK)



- B. Customer managed CMK with AWS generated key material
- C. Customer managed CMK with imported key material
- D. AWS managed data key

**Answer:** B

#### NEW QUESTION 24

- (Exam Topic 1)

A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

- A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
- B. Implement a rate-based rule with AWS WAF
- C. Use AWS Shield to limit the originating traffic hit rate.
- D. Implement the GeoLocation feature in Amazon Route 53.

**Answer:** B

#### NEW QUESTION 25

- (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 now 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 27

- (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 30

- (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. 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 32

- (Exam Topic 1)

A company's architecture requires that its three Amazon EC2 instances run behind an Application Load Balancer (ALB). The EC2 instances transmit sensitive data between each other. Developers use SSL certificates to encrypt the traffic between the public users and the ALB. However, the Developers are unsure of how to encrypt the data in transit between the ALB and the EC2 instances and the traffic between the EC2 instances.

Which combination of activities must the company implement to meet its encryption requirements? (Select TWO)

- A. Configure SSL/TLS on the EC2 instances and configure the ALB target group to use HTTPS
- B. Ensure that all resources are in the same VPC so the default encryption provided by the VPC is used to encrypt the traffic between the EC2 instances.
- C. In the ALB
- D. Select the default encryption to encrypt the traffic between the ALB and the EC2 instances
- E. In the code for the application, include a cryptography library and encrypt the data before sending it between the EC2 instances
- F. Configure AWS Direct Connect to provide an encrypted tunnel between the EC2 instances

**Answer:** BC

### NEW QUESTION 33

- (Exam Topic 1)

A recent security audit identified that a company's application team injects database credentials into the environment variables of an AWS Fargate task. The company's security policy mandates that all sensitive data be encrypted at rest and in transit.

When combination of actions should the security team take to make the application compliant within the security policy? (Select THREE)

- A. Store the credentials securely in a file in an Amazon S3 bucket with restricted access to the application team IAM role. Ask the application team to read the credentials from the S3 object instead.
- B. Create an AWS Secrets Manager secret and specify the key/value pairs to be stored in this secret.
- C. Modify the application to pull credentials from the AWS Secrets Manager secret instead of the environment variables.
- D. Add the following statement to the container instance IAM role policy:

```
{
  "Effect": "Allow",
  "Action": [
    "ssm:GetParameters",
    "secretsmanager:GetSecretValue",
    "kms:Decrypt"
  ],
  "Resource": [
    "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
    "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
  ]
}
```

- E. Add the following statement to the execution role policy.

```
{
  "Effect": "Allow",
  "Action": [
    "ssm:GetParameters",
    "secretsmanager:GetSecretValue",
    "kms:Decrypt"
  ],
  "Resource": [
    "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
    "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
  ]
}
```

- F. Log in to the AWS Fargate instance, create a script to read the secret value from AWS Secret Manager, and inject the environment variable.
- G. Ask the application team to redeploy the application.

**Answer:** BEF

### NEW QUESTION 36

- (Exam Topic 1)

A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use AWS. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary.

What solution should the Engineer use to implement the appropriate access restrictions for the application?

- A. Create a NACL to allow access on TCP port 443 from the 1,500 subsidiary CIDR block ranges. Associate the NACL to both the NLB and EC2 instances.
- B. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range.
- C. Associate the security group to the NLB.
- D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
- E. Create an AWS PrivateLink endpoint service in the parent company account attached to the NLB.
- F. Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoint.
- G. Use AWS PrivateLink interface endpoints in the 1,500 subsidiary AWS accounts to connect to the data processing application.
- H. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range.
- I. Associate the security group with EC2 instances.

**Answer:** D

### NEW QUESTION 38

- (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 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 an 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 me 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 me account level

**Answer:** A

#### NEW QUESTION 43

- (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 bucke
- 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 recuning basis
- F. Use AWS Backup to copy EBS snapshots to Amazon S3.

**Answer:** A

#### NEW QUESTION 45

- (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 kmseGcnerate-DataKcy permission added.
- E. The Lambda execution role must have the kms:Encrypt permission added in the AWS IAM policy.

**Answer:** BC

#### NEW QUESTION 47

- (Exam Topic 1)

An external Auditor finds that a company's user passwords have no minimum length. The company is currently using two identity providers:

- AWS IAM federated with on-premises Active Directory
- Amazon Cognito user pools to accessing an AWS Cloud application developed by the company Which combination o1 actions should the Security Engineer take to solve this issue? (Select TWO.)

- A. Update the password length policy In the on-premises Active Directory configuration.
- B. Update the password length policy In the IAM configuration.
- C. Enforce an IAM policy In Amazon Cognito and AWS IAM with a minimum password length condition.
- D. Update the password length policy in the Amazon Cognito configuration.
- E. Create an SCP with AWS Organizations that enforces a minimum password length for AWS IAM and Amazon Cognito.

**Answer:** AD

#### NEW QUESTION 50

- (Exam Topic 1)

An employee accidentally exposed an AWS access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key.

How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

- A. Analyze AWS CloudTrail for activity.
- B. Analyze Amazon CloudWatch Logs for activity.
- C. Download and analyze the IAM Use report from AWS Trusted Advisor.
- D. Analyze the resource inventory in AWS Config for IAM user activity.
- E. Download and analyze a credential report from IAM.

**Answer:** AD

#### Explanation:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_getting-report.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html)

#### NEW QUESTION 55

- (Exam Topic 1)

A company's application runs on Amazon EC2 and stores data in an Amazon S3 bucket The company wants additional security controls in place to limit the likelihood of accidental exposure of data to external parties

Which combination of actions will meet this requirement? (Select THREE.)

- A. Encrypt the data in Amazon S3 using server-side encryption with Amazon S3 managed encryption keys (SSE-S3)
- B. Encrypt the data in Amazon S3 using server-side encryption with AWS KMS managed encryption keys (SSE-KMS)



- C. Create a new Amazon S3 VPC endpoint and modify the VPC's routing tables to use the new endpoint
- D. Use the Amazon S3 Block Public Access feature.
- E. Configure the bucket policy to allow access from the application instances only
- F. Use a NACL to filter traffic to Amazon S3

**Answer:** BCE

#### NEW QUESTION 57

- (Exam Topic 1)

A company is using AWS Organizations to manage multiple AWS accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an AWS KMS CMK. However, when users try to access the files in the S3 bucket, they get an access denied error.

What should a Security Engineer do to troubleshoot this error? (Select THREE )

- A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK
- B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket
- C. Ensure the CMK was created before the S3 bucket.
- D. Ensure the S3 block public access feature is enabled for the S3 bucket.
- E. Ensure that automatic key rotation is disabled for the CMK
- F. Ensure the SCPs within Organizations allow access to the S3 bucket.

**Answer:** ABF

#### NEW QUESTION 61

- (Exam Topic 1)

While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

What action should be performed to allow the ping to work?

- A. In the security group of the EC2 instance, allow inbound ICMP traffic.
- B. In the security group of the EC2 instance, allow outbound ICMP traffic.
- C. In the VPC's NACL, allow inbound ICMP traffic.
- D. In the VPC's NACL, allow outbound ICMP traffic.

**Answer:** D

#### NEW QUESTION 63

- (Exam Topic 1)

A security engineer is responsible for providing secure access to AWS resources for thousands of developers in a company's corporate identity provider (IdP). The developers access a set of AWS services from the corporate premises using IAM credentials. Due to the volume of requests for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developers are sharing their IAM credentials with others to avoid provisioning delays. This causes concern about overall security for the security engineer.

Which actions will meet the program requirements that address security?

- A. Create an Amazon CloudWatch alarm for AWS CloudTrail Events. Create a metric filter to send a notification when the same set of IAM credentials is used by multiple developers.
- B. Create a federation between AWS and the existing corporate IdP. Leverage IAM roles to provide federated access to AWS resources.
- C. Create a VPN tunnel between the corporate premises and the VPC. Allow permissions to all AWS services only if it originates from corporate premises.
- D. Create multiple IAM roles for each IAM user. Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

**Answer:** B

#### NEW QUESTION 68

- (Exam Topic 1)

A security engineer needs to configure monitoring and auditing for AWS Lambda.

Which combination of actions using AWS services should the security engineer take to accomplish this goal? (Select TWO.)

- A. Use AWS Config to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
- B. Use AWS CloudTrail to implement governance, compliance, operational, and risk auditing for Lambda.
- C. Use Amazon Inspector to automatically monitor for vulnerabilities and perform governance, compliance, operational, and risk auditing for Lambda.
- D. Use AWS Resource Access Manager to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
- E. Use Amazon Macie to discover, classify, and protect sensitive data being executed inside the Lambda function.

**Answer:** AB

#### NEW QUESTION 69

- (Exam Topic 1)

A company is setting up products to deploy in AWS Service Catalog. Management is concerned that when users launch products, elevated IAM privileges will be required to create resources. How should the company mitigate this concern?

- A. Add a template constraint to each product in the portfolio.
- B. Add a launch constraint to each product in the portfolio.
- C. Define resource update constraints for each product in the portfolio.



D. Update the AWS CloudFormation template backing the product to include a service role configuration.

**Answer:** C

#### NEW QUESTION 72

- (Exam Topic 1)

A company has a compliance requirement to rotate its encryption keys on an annual basis. A Security Engineer needs a process to rotate the KMS Customer Master Keys (CMKs) that were created using imported key material.

How can the Engineer perform the key rotation process MOST efficiently?

- A. Create a new CMK, and redirect the existing Key Alias to the new CMK
- B. Select the option to auto-rotate the key
- C. Upload new key material into the existing CMK.
- D. Create a new CMK, and change the application to point to the new CMK

**Answer:** A

#### NEW QUESTION 75

- (Exam Topic 1)

A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee. Even after updating the policy the employee still receives an access denied message.

What is the likely cause of this access denial?

- A. The ACL in the bucket needs to be updated.
- B. The IAM policy does not allow the user to access the bucket
- C. It takes a few minutes for a bucket policy to take effect
- D. The allow permission is being overridden by the deny.

**Answer:** D

#### NEW QUESTION 80

- (Exam Topic 1)

A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.

Which solution meets these criteria?

- A. A customer managed CMK that uses customer provided key material
- B. A customer managed CMK that uses AWS provided key material
- C. An AWS managed CMK
- D. Operating system-native encryption that uses GnuPG

**Answer:** B

#### NEW QUESTION 85

- (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 client
- E. Use client-side encryption and sign the table items
- F. Use the AWS Encryption SDK
- G. Use client-side encryption and sign the table items.

**Answer:** A

#### NEW QUESTION 90

- (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 (NACL) 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 94

- (Exam Topic 2)

You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks.  
 Which of the following service can help in such a scenario  
 Please select:

- A. AWS Trusted Advisor
- B. AWS WAF
- C. AWS Inspector
- D. AWS Config

**Answer: B**

#### Explanation:

The AWS Documentation mentions the following

AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect.

Option A is invalid because this will only give advise on how you can better the security in your AWS account but not protect against threats mentioned in the question.

Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.

Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest

For more information on AWS WAF, please visit the following URL: <https://aws.amazon.com/waf/details>;

The correct answer is: AWS WAF

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 96

- (Exam Topic 2)

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?  
 Please select:

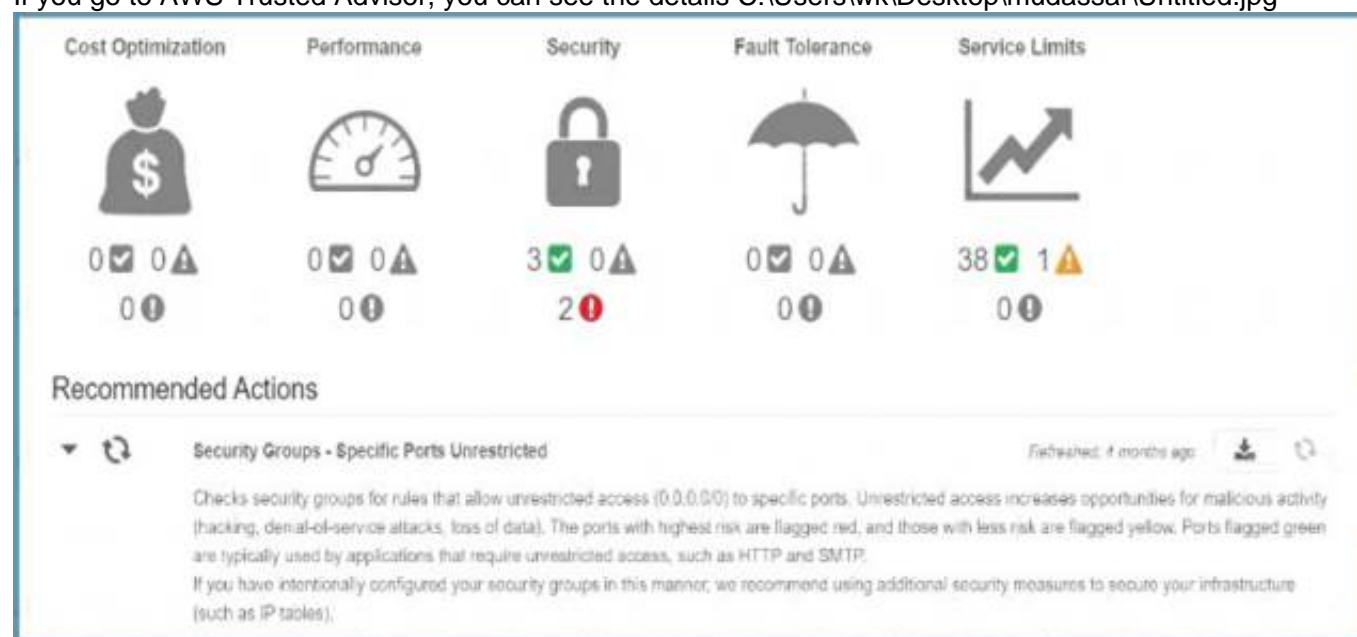
- A. Use AWS Inspector to inspect all the security Groups
- B. Use the AWS Trusted Advisor to see which security groups have compromised access.
- C. Use AWS Config to see which security groups have compromised access.
- D. Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted accessd

**Answer: B**

#### Explanation:

The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

If you go to AWS Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.

Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option Dis partially valid but would just be a maintenance overhead

For more information on the AWS Trusted Advisor, please visit the below URL: <https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices>;

The correct answer is: Use the AWS Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 98

- (Exam Topic 2)

An organization is using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box.

Which of the following actions would resolve this issue?

- A. In CloudTrail, verify that the trail logging bucket has a log prefix configured.
- B. In Amazon SNS, determine whether the "Account spend limit" has been reached for this alert.
- C. In SNS, ensure that the subscription used by these alerts has not been deleted.

D. In CloudWatch, verify that the alarm threshold "consecutive periods" value is equal to, or greater than 1.

**Answer: C**

### NEW QUESTION 103

- (Exam Topic 2)

A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and AWS STS in specific accounts. What is a scalable and efficient approach to meet this requirement?

- A Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

- B Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": *
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "NotAction": [
        "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
      ],
      "Effect": "Deny ",
      "Resource": "*"
    }
  ]
}
```

- C Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```



- D Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": *
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "NotAction": [
    "dynamodb:*", "rds:*", "ec2:*",
    "s3:*", "sts:*"
  ],
  "Effect": "Deny ",
  "Resource": "*"
}
```

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

**Answer:** A

**Explanation:**

It says specific accounts which mean specific governed OUs under your organization and you apply specific service control policy to these OUs.

**NEW QUESTION 106**

- (Exam Topic 2)

A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?

Please select:

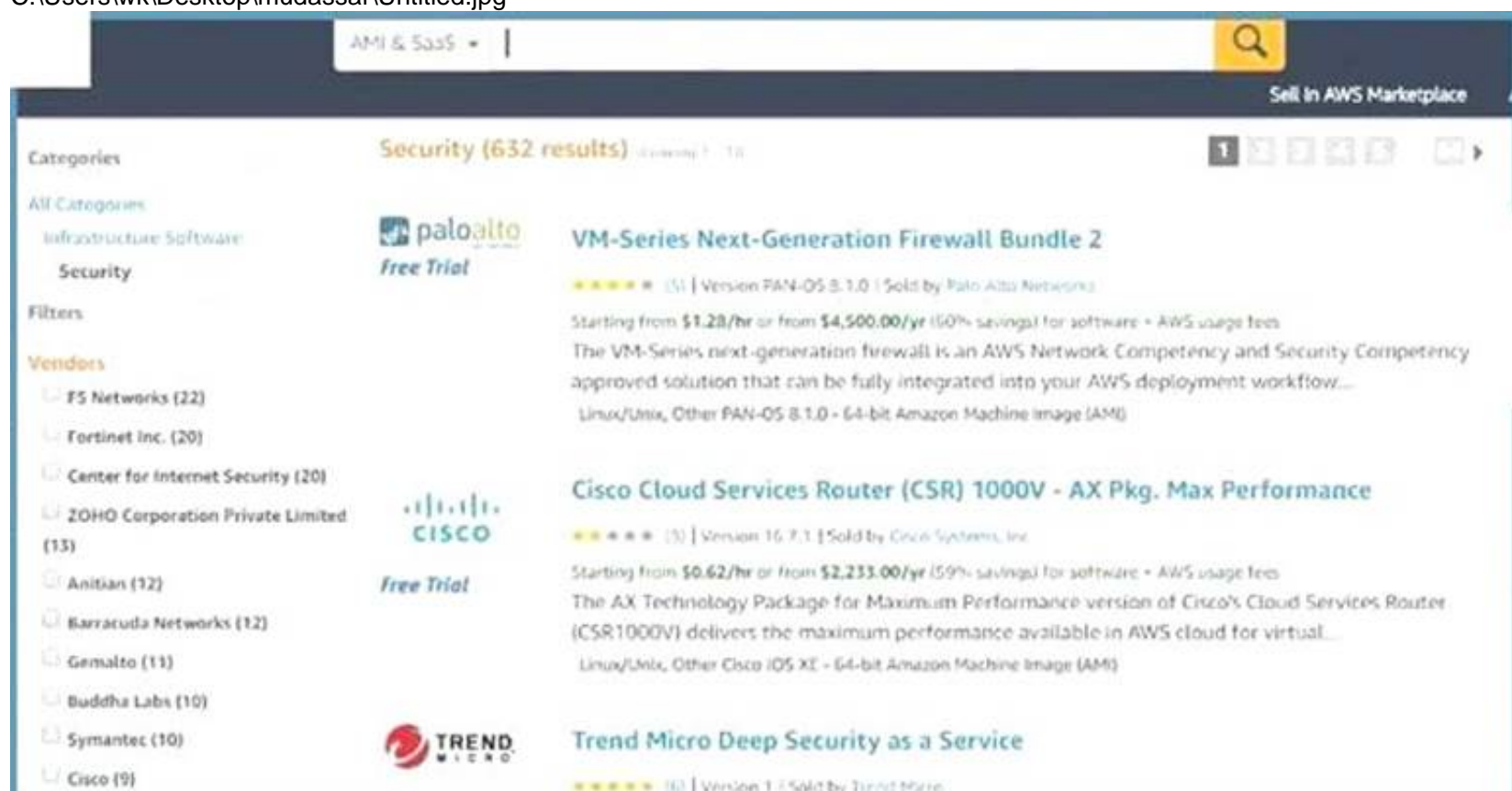
- A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC  
 B. Use a custom solution available in the AWS Marketplace  
 C. Use VPC Flow logs to detect the issues and flag them accordingly.  
 D. Use AWS Cloudwatch to monitor all traffic

**Answer:** B

**Explanation:**

Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.

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





Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL [https://d1.awsstatic.com/Marketplace/security/AWSMP\\_Security\\_Solution%20Overview.pdf](https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%20Overview.pdf)

For more information on using custom security solutions please visit the below URL: [https://d1.awsstatic.com/Marketplace/security/AWSMP\\_Security\\_Solution%20Overview.pdf](https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%20Overview.pdf)

The correct answer is: Use a custom solution available in the AWS Marketplace Submit your Feedback/Queries to our Experts

#### NEW QUESTION 111

- (Exam Topic 2)

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.

Which steps should be taken to troubleshoot the issue? (Choose two.)

- A. Use an EC2 run command to confirm that the “awslogs” service is running on all instances.
- B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
- C. Check whether any application log entries were rejected because of invalid time stamps by reviewing/var/cwlogs/rejects.log.
- D. Check that the trust relationship grants the service “cwlogs.amazonaws.com” permission to write objects to the Amazon S3 staging bucket.
- E. Verify that the time zone on the application servers is in UTC.

**Answer:** AB

#### Explanation:

EC2 run command - can run scripts, install software, collect metrics and log files, manage patches and more. Bringing these two services together - can create CloudWatch Events rules that use EC2 Run Command to perform actions on EC2 instances or on-premises servers.

#### NEW QUESTION 113

- (Exam Topic 2)

A Security Engineer is trying to determine whether the encryption keys used in an AWS service are in compliance with certain regulatory standards.

Which of the following actions should the Engineer perform to get further guidance?

- A. Read the AWS Customer Agreement.
- B. Use AWS Artifact to access AWS compliance reports.
- C. Post the question on the AWS Discussion Forums.
- D. Run AWS Config and evaluate the configuration outputs.

**Answer:** A

#### Explanation:

<https://aws.amazon.com/artifact/>

#### NEW QUESTION 117

- (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 119

- (Exam Topic 2)

The Accounting department at Example Corp. has made a decision to hire a third-party firm, AnyCompany, to monitor Example Corp.'s AWS account to help optimize costs.

The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. AWS resources. The Engineer has created an IAM role and granted permission to AnyCompany's AWS account to assume this role.

When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.

What steps should the Engineer perform to prevent this outcome?

- A. Create an IAM user and generate a set of long-term credential
- B. Provide the credentials to AnyCompany. Monitor access in IAM access advisor and plan to rotate credentials on a recurring basis.
- C. Request an external ID from AnyCompany and add a condition with sts:ExternalId to the role's trust policy.
- D. Require two-factor authentication by adding a condition to the role's trust policy with aws:MultiFactorAuthPresent.
- E. Request an IP range from AnyCompany and add a condition with aws:SourceIp to the role's trust policy.

**Answer:** B

#### NEW QUESTION 124

- (Exam Topic 2)

While analyzing a company's security solution, a Security Engineer wants to secure the AWS account root user.

What should the Security Engineer do to provide the highest level of security for the account?

- A. Create a new IAM user that has administrator permissions in the AWS account
- B. Delete the password for the AWS account root user.

- C. Create a new IAM user that has administrator permissions in the AWS account
- D. Modify the permissions for the existing IAM users.
- E. Replace the access key for the AWS account root user
- F. Delete the password for the AWS account root user.
- G. Create a new IAM user that has administrator permissions in the AWS account
- H. Enable multi-factor authentication for the AWS account root user.

**Answer:** D

**Explanation:**

If you continue to use the root user credentials, we recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

**NEW QUESTION 125**

- (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 129**

- (Exam Topic 2)

The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.

How can the InfoSec team ensure compliance with this mandate?

- A. Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
- B. Patch all running instances by using AWS Systems Manager.
- C. Deploy AWS Config rules and check all running instances for compliance.
- D. Define a metric filter in Amazon CloudWatch Logs to verify compliance.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/config/latest/developerguide/approved-amis-by-id.html>

**NEW QUESTION 134**

- (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 rotate
- G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

**Answer:** CE

**NEW QUESTION 137**

- (Exam Topic 2)

Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved? Please select:

- A. Enable logging on the KMS service
- B. Enable a trail in Cloudtrail
- C. Enable Cloudwatch logs
- D. Use Cloudwatch metrics

**Answer:** B

**Explanation:**

The AWS Documentation states the following

AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.

Option A is invalid because logging is not possible in the KMS service

Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL

<https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html> The correct answer is: Enable a trail in Cloudtrail

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 142

- (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 144

- (Exam Topic 2)

A Development team has asked for help configuring the IAM roles and policies in a new AWS account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).

Which of the following will allow the team to manage AWS KMS permissions in IAM without the complexity of editing individual key policies?

- A. The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.
- B. Newly created CMKs must have a key policy that allows the root principal to perform all actions.
- C. Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
- D. Newly created CMKs must mirror the IAM policy of the KMS key administrator.

**Answer: B**

#### Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enable>

#### NEW QUESTION 147

- (Exam Topic 2)

The AWS Systems Manager Parameter Store is being used to store database passwords used by an AWS Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an AWS KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.

Which of the following actions will resolve the access denied error?

- A. Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.
- B. Update the Lambda configuration to launch the function in a VPC.
- C. Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
- D. Add lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.

**Answer: C**

#### Explanation:

[https://docs.amazonaws.cn/en\\_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizing](https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizing)

#### NEW QUESTION 151

- (Exam Topic 2)

Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?

Please select:

- A. Turn on Cloud trail and carry out the penetration test
- B. Turn on VPC Flow Logs and carry out the penetration test
- C. Submit a request to AWS Support
- D. Use a custom AWS Marketplace solution for conducting the penetration test

**Answer: C**

#### Explanation:

This concept is given in the AWS Documentation

How do I submit a penetration testing request for my AWS resources? Issue

I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?

Resolution

Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.

AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.

If your request is approved, you'll receive an authorization number.

Option A,B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests

For more information on penetration testing, please visit the below URL

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

\* <https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/> (

The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

### NEW QUESTION 153

- (Exam Topic 2)

What is the function of the following AWS Key Management Service (KMS) key policy attached to a customer master key (CMK)?

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "workmail.us-west-2.amazonaws.com",
        "ses.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.

B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and AWS.

C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and the request comes from WorkMail or SES in the specified region.

D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

**Answer: C**

### NEW QUESTION 156

- (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 159**

- (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 161**

- (Exam Topic 2)

An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.

Which steps should be taken to investigate the suspected compromise? (Choose three.)

- A. Detach the elastic network interface from the EC2 instance.
- B. Initiate an Amazon Elastic Block Store volume snapshot of all volumes on the EC2 instance.
- C. Disable any Amazon Route 53 health checks associated with the EC2 instance.
- D. De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.
- E. Attach a security group that has restrictive ingress and egress rules to the EC2 instance.
- F. Add a rule to an AWS WAF to block access to the EC2 instance.

**Answer:** BDE

**Explanation:**

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

**NEW QUESTION 164**

- (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 168**

- (Exam Topic 2)

An AWS Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.

Which of the following explains why the logs are not available?

- A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
- B. The Lambda function was executed by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
- C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
- D. The version of the Lambda function that was executed was not current.

**Answer:** A

**NEW QUESTION 173**

- (Exam Topic 2)

The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using AWS CloudFormation templates with EC2 Auto Scaling groups:

- Have the EC2 instances bootstrapped to connect to a backend database.
- Ensure that the database credentials are handled securely.
- Ensure that retrievals of database credentials are logged.

Which of the following is the MOST efficient way to meet these requirements?

- A. Pass databases credentials to EC2 by using CloudFormation stack parameters with the property set to tru
- B. Ensure that the instance is configured to log to Amazon CloudWatch Logs.
- C. Store database passwords in AWS Systems Manager Parameter Store by using SecureString parameters.Set the IAM role for the EC2 instance profile to allow access to the parameters.
- D. Create an AWS Lambda that ingests the database password and persists it to Amazon S3 with server-side encryptio
- E. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.
- F. Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance.Ensure that the instance is configured to log to Amazon CloudWatch Logs.

**Answer: B**

#### NEW QUESTION 177

- (Exam Topic 2)

A Security Administrator is performing a log analysis as a result of a suspected AWS account compromise. The Administrator wants to analyze suspicious AWS CloudTrail log files but is overwhelmed by the volume of audit logs being generated.

What approach enables the Administrator to search through the logs MOST efficiently?

- A. Implement a “write-only” CloudTrail event filter to detect any modifications to the AWS account resources.
- B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
- C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
- D. Enable Amazon S3 event notifications to trigger an AWS Lambda function that sends an email alarm when there are new CloudTrail API entries.

**Answer: C**

#### NEW QUESTION 180

- (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 185**

- (Exam Topic 2)

A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys. Which solution meets these requirements?

- A. Use AWS KMS with AWS managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.
- B. Use KMS with AWS imported key material and then use the DeleteImportedKeyMaterial API to remove the key material if necessary.
- C. Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.
- D. Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.

**Answer: C**

**Explanation:**

<https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-delete-key-material.html>

**NEW QUESTION 186**

- (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 tool 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 190**

- (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 193**

- (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 it
- B. Perform inspection within proxy software on the EC2 instance.
- C. Configure the host-based agent on each EC2 instance within the VPC
- D. Perform inspection within the host-based agent.
- E. Enable VPC Flow Logs for all subnets in the VPC
- 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 VPC
- 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 194**

- (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 198**

- (Exam Topic 2)

Your company has a set of resources defined in the AWS Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?

Please select:

- A. Create a powershell script using the AWS CLI
- B. Query for all resources with the tag of production.
- C. Create a bash shell script with the AWS CLI
- D. Query for all resources in all region



- E. Store the results in an S3 bucket.
- F. Use Cloud Trail to get the list of all resources
- G. Use AWS Config to get the list of all resources

**Answer: D**

**Explanation:**

The most feasible option is to use AWS Config. When you turn on AWS Config, you will get a list of resources defined in your AWS Account. A sample snapshot of the resources dashboard in AWS Config is shown below C:\Users\wk\Desktop\mudassar\Untitled.jpg

Resources	
Total resource count	131
Top 10 resource types	Total
 IAM Policy	45
 IAM Role	40
 EC2 Subnet	7
 EC2 SecurityGroup	6
 EC2 RouteTable	6
 EC2 VPC	4
 EC2 NetworkAcl	4

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.

Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on AWS Config, please visit the below URL: <https://docs.aws.amazon.com/config/latest/developerguide/how-does-confie-work.html>

The correct answer is: Use AWS Config to get the list of all resources Submit your Feedback/Queries to our Experts

**NEW QUESTION 200**

- (Exam Topic 2)

A company plans to move most of its IT infrastructure to AWS. They want to leverage their existing on-premises Active Directory as an identity provider for AWS. Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with AWS? (Choose two.)

- A. Create IAM roles with permissions corresponding to each Active Directory group.
- B. Create IAM groups with permissions corresponding to each Active Directory group.
- C. Configure Amazon Cloud Directory to support a SAML provider.
- D. Configure Active Directory to add relying party trust between Active Directory and AWS.
- E. Configure Amazon Cognito to add relying party trust between Active Directory and AWS.

**Answer: AD**

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-activ>

**NEW QUESTION 202**

- (Exam Topic 2)

During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.

What could have been done to detect and automatically remediate the incident?

- A. Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to AWS CloudTrail, and revoke the new API keys for the root user.
- B. Using AWS Config, create a config rule that detects when AWS CloudTrail is disabled, as well as any calls to the root user create-api-ke
- C. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.
- D. Using Amazon CloudWatch, create a CloudWatch event that detects AWS CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API key
- E. Then use a Lambda function to enable AWS CloudTrail and deactivate the root API keys.
- F. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API key
- G. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/config/latest/developerguide/cloudtrail-enabled.html> <https://docs.aws.amazon.com/config/latest/developerguide/iam-root-access-key->

check.html

**NEW QUESTION 204**

- (Exam Topic 2)

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards. The mail application should be configured to connect to which of the following endpoints and corresponding ports?

- A. email.us-east-1.amazonaws.com over port 8080
- B. email-pop3.us-east-1.amazonaws.com over port 995
- C. email-smtp.us-east-1.amazonaws.com over port 587
- D. email-imap.us-east-1.amazonaws.com over port 993

**Answer: C**

**Explanation:**

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html>

**NEW QUESTION 208**

- (Exam Topic 2)

A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.

The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.

How can the Security Engineer address the issue?

- A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed
- B. Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications
- C. Use GuardDuty filters with auto archiving enabled to close the findings
- D. Create an AWS Lambda function that closes the finding whenever a new occurrence is reported

**Answer: B**

**Explanation:**

Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per AWS account per region.

References:

**NEW QUESTION 213**

- (Exam Topic 2)

A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).

What mechanism will allow the company to implement all required network rules without incurring additional cost?

- A. Configure AWS WAF rules to implement the required rules.
- B. Use the operating system built-in, host-based firewall to implement the required rules.
- C. Use a NAT gateway to control ingress and egress according to the requirements.
- D. Launch an EC2-based firewall product from the AWS Marketplace, and implement the required rules in that product.

**Answer: B**

**NEW QUESTION 215**

- (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 218**

- (Exam Topic 2)

A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.

An operational safety policy requires that access to specific credentials is independently auditable. What is the MOST cost-effective way to manage the storage of credentials?

- A. Use AWS Systems Manager to store the credentials as Secure Strings Parameter
- B. Secure by using an AWS KMS key.
- C. Use AWS Key Management System to store a master key, which is used to encrypt the credential

- D. The encrypted credentials are stored in an Amazon RDS instance.
- E. Use AWS Secrets Manager to store the credentials.
- F. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/systems-manager/latest/userguide/parameter-store-advanced-parameters.html>

**NEW QUESTION 221**

- (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 222**

- (Exam Topic 2)

A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.

What is the MOST efficient way to manage access control for the KMS CMK?

- A. Use KMS grants to manage key acces
- B. Programmatically create and revoke grants to manage vendor access.
- C. Use an IAM role to manage key acces
- D. Programmatically update the IAM role policies to manage vendor access.
- E. Use KMS key policies to manage key acces
- F. Programmatically update the KMS key policies to manage vendor access.
- G. Use delegated access across AWS accounts by using IAM roles to manage key access. Programmatically update the IAM trust policy to manage cross-account vendor access.

**Answer:** A

**NEW QUESTION 223**

- (Exam Topic 2)

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.

How should the Lambda function be given access to the DynamoDB table? Please select:

- A. Create a VPC endpoint for DynamoDB within a VP
- B. Configure the Lambda function to access resources in the VPC.
- C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table. Attach the poll to the DynamoDB table.
- D. Create an IAM user with permissions to write to the DynamoDB tabl
- E. Store an access key for that user in the Lambda environment variables.
- F. Create an IAM service role with permissions to write to the DynamoDB tabl
- G. Associate that role with the Lambda function.

**Answer:** D

**Explanation:**

The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function

The AWS Documentation additionally mentions the following

Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.

If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.

Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB

Option B is invalid because resources policies are present for resources such as S3 and KMS, but not AWS Lambda

Option C is invalid because AWS Roles should be used and not IAM Users

For more information on the Lambda permission model, please visit the below URL: <https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html>

The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Exp

**NEW QUESTION 228**

- (Exam Topic 2)

A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year.

What can be done to implement the above policy?

- A. Enable automatic key rotation annually for the CMK.
- B. Use AWS Command Line Interface to create an AWS Lambda function to rotate the existing CMK annually.
- C. Import new key material to the existing CMK and manually rotate the CMK.
- D. Create a new CMK, import new key material to it, and point the key alias to the new CMK.

**Answer: D**

**Explanation:**

[https://docs.aws.amazon.com/en\\_pv/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually](https://docs.aws.amazon.com/en_pv/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually)

"You might prefer to rotate keys manually so you can control the rotation frequency. It's also a good solution for CMKs that are not eligible for automatic key rotation, such as asymmetric CMKs, CMKs in custom key stores and CMKs with imported key material. Because the new CMK is a different resource from the current CMK, it has a different key ID and ARN. When you change CMKs, you need to update references to the CMK ID or ARN in your applications. Aliases, which associate a friendly name with a CMK, make this process easier. Use an alias to refer to a CMK in your applications. Then, when you want to change the CMK that the application uses, change the target CMK of the alias. To update the target CMK of an alias, use UpdateAlias operation in the AWS KMS API. "

**NEW QUESTION 230**

- (Exam Topic 2)

A company hosts a critical web application on the AWS Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?

Please select:

- A. Consider using the AWS Shield Service
- B. Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.
- C. Consider using the AWS Shield Advanced Service
- D. Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

**Answer: C**

**Explanation:**

Option A is invalid because the normal AWS Shield Service will not help in immediate action against a DDos attack. This can be done via the AWS Shield Advanced Service

Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDos attacks.

Option D is invalid because this is a logging service for AWS Services but cannot specifically protect against DDos attacks.

The AWS Documentation mentions the following

AWS Shield Advanced provides enhanced protections for your applications running on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. AWS Shield Advanced is available to AWS Business Support and AWS Enterprise Support customers. AWS Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDos attacks. AWS Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDos Response Team (DRT) 24X7 to manage and mitigate their application layer DDos attacks.

For more information on AWS Shield, please visit the below URL: <https://aws.amazon.com/shield/faqs>;

The correct answer is: Consider using the AWS Shield Advanced Service Submit your Feedback/Queries to our Experts

**NEW QUESTION 232**

- (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 234**

- (Exam Topic 2)

A company runs an application on AWS that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel. How can the Security Engineer protect this workload so that only employees can access it?

- A. Add each employee's home IP address to the security group for the application so that only those users can access the workload.
- B. Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.
- C. Use a VPN appliance from the AWS Marketplace for users to connect to, and restrict workload access to traffic from that appliance.
- D. Route all traffic to the workload through AWS WA
- E. Add each employee's home IP address into an AWS WAF rule, and block all other traffic.



**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/what-is.html>

**NEW QUESTION 238**

- (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 240**

- (Exam Topic 2)

An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities. How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

- A. Use a filter in AWS CloudTrail to exclude the IP addresses of the Security team's EC2 instances.
- B. Add the Elastic IP addresses of the Security team's EC2 instances to a trusted IP list in Amazon GuardDuty.
- C. Install the Amazon Inspector agent on the EC2 instances that the Security team uses.
- D. Grant the Security team's EC2 instances a role with permissions to call Amazon GuardDuty API operations.

**Answer:** B

**Explanation:**

Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per AWS account per region. Threat lists consist of known malicious IP addresses. GuardDuty generates findings based on threat lists. At any given time, you can have up to six uploaded threat lists per AWS account per region. [https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_upload\\_lists.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html)

**NEW QUESTION 242**

- (Exam Topic 2)

An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer. There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses AWS WAF. The application is currently experiencing a volumetric attack whereby the attacker is exploiting a bug in a popular mobile game.

The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0)

What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

- A. Create a rule in AWS WAF rules with conditions that block requests based on the presence of ExampleGame/1.22 in the User-Agent header
- B. Create a geographic restriction on the CloudFront distribution to prevent access to the application from most geographic regions
- C. Create a rate-based rule in AWS WAF to limit the total number of requests that the web application services.
- D. Create an IP-based blacklist in AWS WAF to block the IP addresses that are originating from requests that contain ExampleGame/1.22 in the User-Agent header.

**Answer:** A

**Explanation:**

Since all the attack has http header- User-Agent set to string: Mozilla/5.0 (compatible; ExampleCorp;) it would be much more easier to block these attack by simply denying traffic with the header match . HTH ExampleGame/1.22; Mobile/1.0)

**NEW QUESTION 244**

- (Exam Topic 3)

A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that I is never accessible directly.

How should the security engineer build the MOST secure solution?

- A. Add an origin custom header Set the viewer protocol policy to HTTP and HTTPS Set the origin protocol pokey to HTTPS only Update the application to validate the CloudFront custom header
- B. Add an origin custom header Set the viewer protocol policy to HTTPS only Set the origin protocol policy to match viewer Update the application to validate the CloudFront custom header.
- C. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS Set the origin protocol policy to HTTP only Update the application to validate the CloudFront custom header.
- D. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTP
- E. Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header

**Answer:** D

**NEW QUESTION 246**

- (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 groupCheck 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 251**

- (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 IAM role with a Team tag key  
 E. and use the team name in the tag value  
 F. 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": {
        "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 252

- (Exam Topic 3)

You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.

Please select:

- A. Check to see if the right role has been assigned to the EC2 instances  
 B. Check to see if the IAM user has the right permissions for EC2  
 C. Ensure that agent is running on the instances.  
 D. Check the Instance status by using the Health API.

**Answer: ACD**

### Explanation:

For ensuring that the instances are configured properly you need to ensure the following:

- 1) You installed the latest version of the SSM Agent on your instance
- 2) Your instance is configured with an AWS Identity and Access Management (IAM) role that enables the instance to communicate with the Systems Manager API
- 3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances:
  - The status of one or more instances
  - The last time the instance sent a heartbeat value
  - The version of the SSM Agent
  - The operating system
  - The version of the EC2Config service (Windows)
  - The status of the EC2Config service (Windows)

Option B is invalid because IAM users are not supposed to be directly granted permissions to EC2 Instances. For more information on troubleshooting AWS SSM, please visit the following URL:  
<https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remote-commands.html>

The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.

Submit your Feedback/Queries to our Experts



### NEW QUESTION 255

- (Exam Topic 3)

A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS. What could be the strategy to adopt for managing the accounts.  
Please select:

- A. Use multiple VPCs in the account each VPC for each department
- B. Use multiple IAM groups, each group for each department
- C. Use multiple IAM roles, each group for each department
- D. Use multiple AWS accounts, each account for each department

**Answer: D**

#### Explanation:

A recommendation for this is given in the AWS Security best practices C:\Users\wk\Desktop\mudassar\Untitled.jpg

**Design your AWS account strategy to maximize security and follow your business and governance requirements. Table 3 discusses possible strategies.**

Business Requirement	Proposed Design	Comments
Centralized security management	Single AWS account	Centralize information security management and minimize overhead.
Separation of production, development, and testing environments	Three AWS accounts	Create one AWS account for production services, one for development, and one for testing.
Multiple autonomous departments	Multiple AWS accounts	Create separate AWS accounts for each autonomous part of the organization. You can assign permissions and policies under each account.
Centralized security management with multiple autonomous independent projects	Multiple AWS accounts	Create a single AWS account for common project resources (such as DNS services, Active Directory, CMS etc.). Then create separate AWS accounts per project. You can assign permissions and policies under each project account and grant access to resources across accounts.

Table 3: AWS Account Strategies

Option A is incorrect since this would be applicable for resources in a VPC Options B and C are incorrect since operationally it would be difficult to manage For more information on AWS Security best practices please refer to the below URL

[https://d1.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Best\\_Practices.pdf](https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)

The correct answer is: Use multiple AWS accounts, each account for each department Submit your Feedback/Queries to our Experts

### NEW QUESTION 260

- (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 ta
- 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 employe 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 261

- (Exam Topic 3)

A company has set up EC2 instances on the AW5 Cloud. There is a need to see all the IP addresses which are accessing the EC2 Instances. Which service can help achieve this?  
Please select:

- A. Use the AWS Inspector service
- B. Use AWS VPC Flow Logs
- C. Use Network ACL's
- D. Use Security Groups

**Answer: B**



#### Explanation:

The AWS Documentation mentions the foil

A flow log record represents a network flow in your flow log. Each record captures the network flow for a specific 5-tuple, for a specific capture window. A 5-tuple is a set of five different values that specify the source, destination, and protocol for an internet protocol (IP) flow.

Options A,C and D are all invalid because these services/tools cannot be used to get the the IP addresses which are accessing the EC2 Instances

For more information on VPC Flow Logs please visit the URL <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

The correct answer is: Use AWS VPC Flow Logs Submit your Feedback/Queries to our Experts

#### NEW QUESTION 265

- (Exam Topic 3)

You currently have an S3 bucket hosted in an AWS Account. It holds information that needs be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.

Please select:

- A. Ensure an IAM role is created which can be assumed by the partner account.
- B. Ensure an IAM user is created which can be assumed by the partner account.
- C. Ensure the partner uses an external id when making the request
- D. Provide the ARN for the role to the partner account
- E. Provide the Account Id to the partner account
- F. Provide access keys for your account to the partner account

**Answer:** ACD

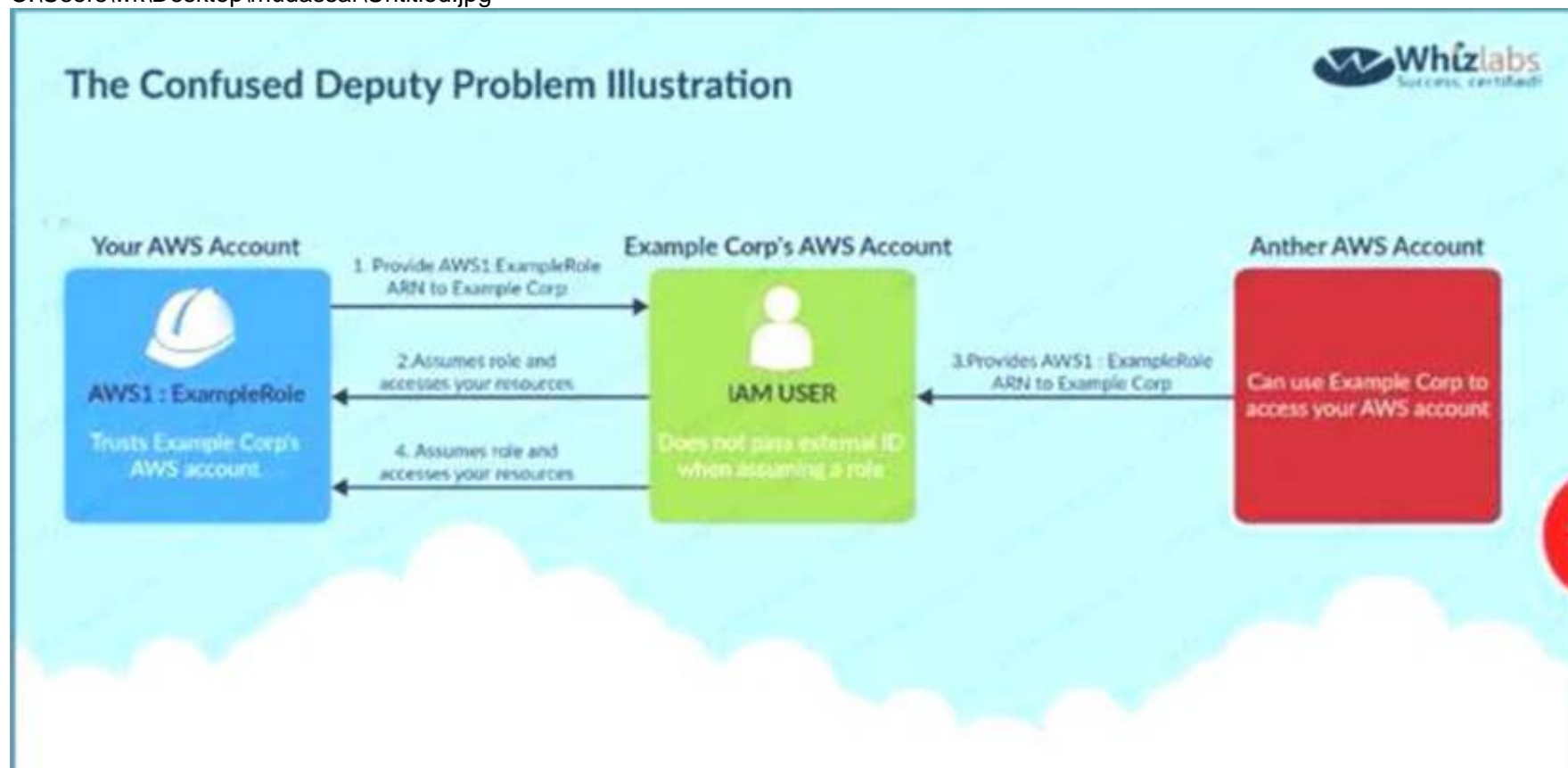
#### Explanation:

Option B is invalid because Roles are assumed and not IAM users

Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner

The below diagram from the AWS documentation showcases an example on this wherein an IAM role and external ID is used to access an AWS account resources

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



For more information on creating roles for external ID'S please visit the following URL:

The correct answers are: Ensure an IAM role is created which can be assumed by the partner account. Ensure the partner uses an external id when making the request Provide the ARN for the role to the partner account

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 266

- (Exam Topic 3)

You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved?

Please select:

- A. Add the keys to the backend distribution.
- B. Add the keys to the S3 bucket
- C. Create pre-signed URL's
- D. Use AWS Access keys

**Answer:** C

#### Explanation:

Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket. Option D is invalid because this is used for programmatic access to AWS resources

You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the AWS Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers) Topics

- Creating CloudFront Key Pairs for Your Trusted Signers
- Reformatting the CloudFront Private Key (.NET and Java Only)
- Adding Trusted Signers to Your Distribution
- Verifying that Trusted Signers Are Active (Optional) 1 Rotating CloudFront Key Pairs

To create signed URLs or signed cookies, you need at least one AWS account that has an active CloudFront key pair. This account is known as a trusted signer.

The trusted signer has two purposes:

- As soon as you add the AWS account ID for your trusted signer to your distribution, CloudFront starts to require that users use signed URLs or signed cookies to access your objects.
- ' When you create signed URLs or signed cookies, you use the private key from the trusted signer's key pair to sign a portion of the URL or the cookie. When someone requests a restricted object CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed. For more information on Cloudfront private trusted content please visit the following URL:
- <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-trusted-s> The correct answer is: Create pre-signed URL's Submit your Feedback/Queries to our Experts

#### NEW QUESTION 269

- (Exam Topic 3)

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

- A. Use AWS Config to ensure that the servers have no critical flaws.
- B. Use AWS Inspector to ensure that the servers have no critical flaws.
- C. Use AWS inspector to patch the servers
- D. Use AWS SSM to patch the servers

**Answer:** BD

#### Explanation:

The AWS Documentation mentions the following on AWS Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers Option C is invalid because the AWS Inspector service is not used to patch servers

For more information on AWS Inspector, please visit the following URL: <https://aws.amazon.com/inspector>

Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.

For more information on the Systems Manager, please visit the following URL: <https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html>

The correct answers are: Use AWS Inspector to ensure that the servers have no critical flaws.. Use AWS SSM to patch the servers

(

#### NEW QUESTION 272

- (Exam Topic 3)

Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which three IAM best practices should you consider implementing?  
Please select:

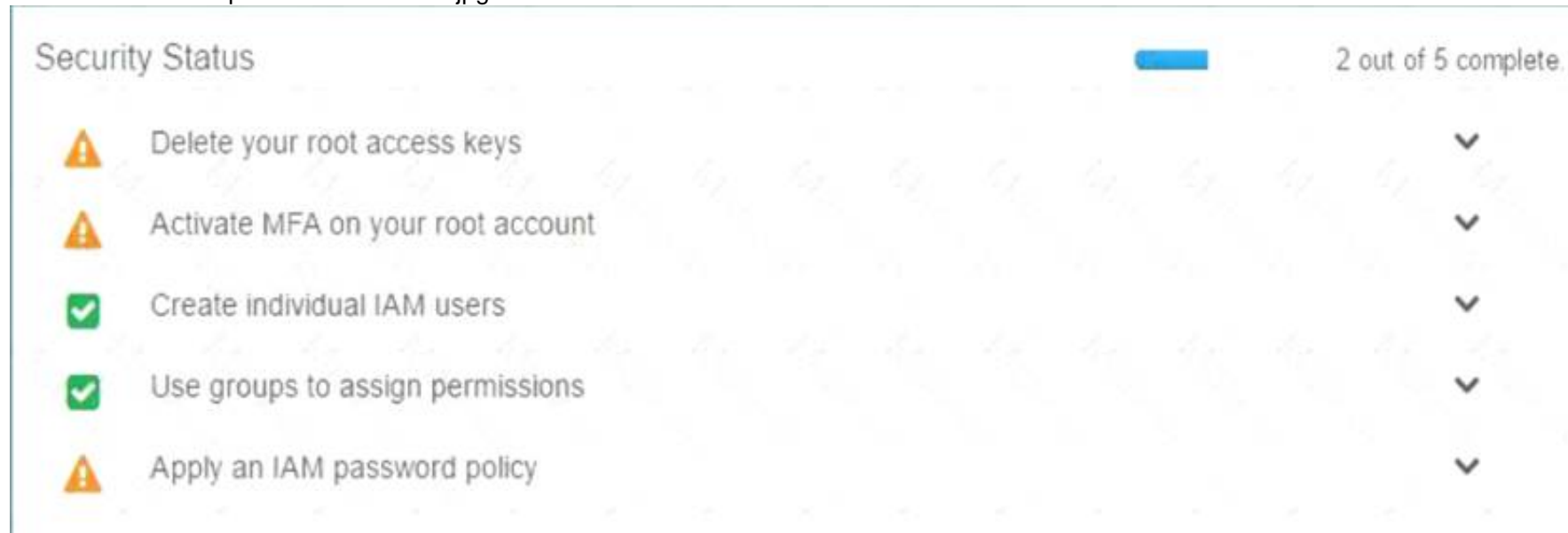
- A. Create individual IAM users
- B. Configure MFA on the root account and for privileged IAM users
- C. Assign IAM users and groups configured with policies granting least privilege access
- D. Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate

**Answer:** ABC

#### Explanation:

When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.

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



Option D is invalid because as per the dashboard, this is not part of the security recommendation For more information on best security practices please visit the URL:

<https://aws.amazon.com/whitepapers/aws-security-best-practices>;

The correct answers are: Create individual IAM users, Configure MFA on the root account and for privileged IAM users. Assign IAM users and groups configured with policies granting least privilege access

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 273

- (Exam Topic 3)

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol.

There is a security mandate that all traffic between the client and the EC2 Instances need to be secure. How would you accomplish this?  
Please select:

- A. Use an Application Load balancer and terminate the SSL connection at the ELB
- B. Use a Classic Load balancer and terminate the SSL connection at the ELB
- C. Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
- D. Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

**Answer:** D

**Explanation:**

Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the EC2 Instances.

Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application. Option B is incorrect since encryption is required until the EC2 Instance

For more information on HTTPS listeners for classic load balancers, please refer to below URL

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html>

The correct answer is: Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances Submit your Feedback/Queries to our Experts

**NEW QUESTION 274**

- (Exam Topic 3)

A development team is using an AWS Key Management Service (AWS KMS) CMK to try to encrypt and decrypt a secure string parameter from AWS Systems Manager Parameter Store. However, the development team receives an error message on each attempt.

Which issues that are related to the CMK could be reasons for the error? (Select TWO.)

- A. The CMK that is used in the attempt does not exist.
- B. The CMK that is used in the attempt needs to be rotated.
- C. The CMK that is used in the attempt is using the CMK's key ID instead of the CMK ARN.
- D. The CMK that is used in the attempt is not enabled.
- E. The CMK that is used in the attempt is using an alias.

**Answer:** AD

**NEW QUESTION 275**

- (Exam Topic 3)

An application running on EC2 instances in a VPC must access sensitive data in the data center. The access must be encrypted in transit and have consistent low latency. Which hybrid architecture will meet these requirements?

Please select:

- A. Expose the data with a public HTTPS endpoint.
- B. A VPN between the VPC and the data center over a Direct Connect connection
- C. A VPN between the VPC and the data center.
- D. A Direct Connect connection between the VPC and data center

**Answer:** B

**Explanation:**

Since this is required over a consistency low latency connection, you should use Direct Connect. For encryption, you can make use of a VPN

Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.

Option C is invalid because low latency is a key requirement Option D is invalid because only Direct Connect will not suffice

For more information on the connection options please see the below Link: <https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharint>

The correct answer is: A VPN between the VPC and the data center over a Direct Connect connection Submit your Feedback/Queries to our Experts

**NEW QUESTION 276**

- (Exam Topic 3)

A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch

What should the security engineer do next to meet this requirement?

Within AWS Key Management Service (AWS KMS) specify the deletion time of the key material during CMK creation AWS KMS will automatically create a CloudWatch.

Create an Amazon Eventbridge (Amazon CloudWatch Events) rule to look for API calls of DeleteAlias Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) messages to the company Add the Lambda functions as the target of the Eventbridge (CloudWatch Events) rule.

Create an Amazon EventBridge (Amazon CloudWatch Events) rule to look for API calls of DisableKey and ScheduleKeyDeletion. Create an AWS Lambda function to generate the alarm and send the notification to the company. Add the lambda function as the target of the SNS policy.

- A. Use inbound rule 100 to allow traffic on TCP port 443 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443
- B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port 443
- C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443
- D. Use inbound rule 100 to deny traffic on TCP port 3306 Use inbound rule 200 to allow traffic on TCP port 443 Use outbound rule 100 to allow traffic on TCP port 443

**Answer:** A

**NEW QUESTION 281**

- (Exam Topic 3)

An ecommerce website was down for 1 hour following a DDoS attack Users were unable to connect to the website during the attack period. The ecommerce

company's security team is worried about future potential attacks and wants to prepare for such events. The company needs to minimize downtime in its response to similar attacks in the future.

Which steps would help achieve this? (Select TWO)

- A. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.
- B. Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack.
- C. Use VPC Flow Logs to monitor network traffic and an AWS Lambda function to automatically block an attacker's IP using security groups.
- D. Set up an Amazon CloudWatch Events rule to monitor the AWS CloudTrail events in real time, use AWS Config rules to audit the configuration, and use AWS Systems Manager for remediation.
- E. Use AWS WAF to create rules to respond to such attacks.

**Answer: CE**

#### **NEW QUESTION 286**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SCS-C01 Practice Test Here](#)**