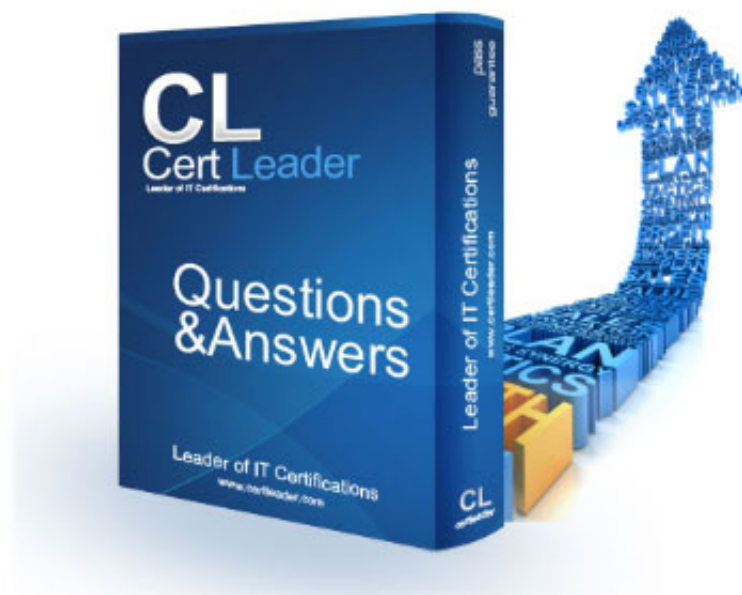


## SCS-C01 Dumps

### AWS Certified Security- Specialty

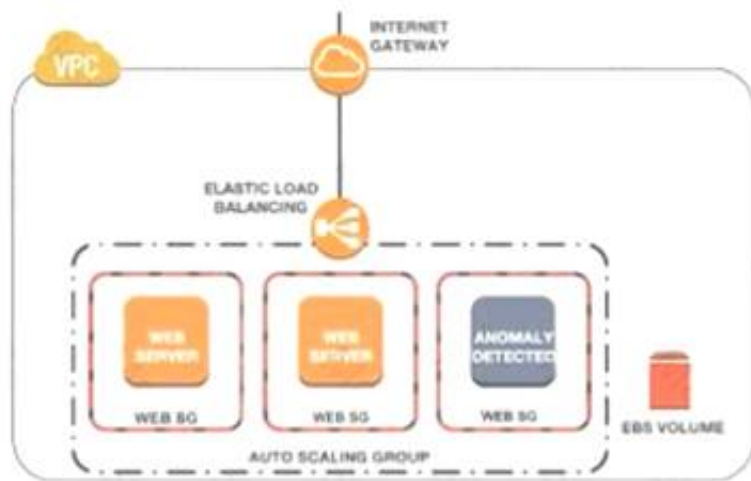
<https://www.certleader.com/SCS-C01-dumps.html>



### NEW QUESTION 1

- (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 image 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 2

- (Exam Topic 1)

A company has a VPC with several Amazon EC2 instances behind a NAT gateway. The company's security policy states that all network traffic must be logged and must include the original source and destination IP addresses. The existing VPC Flow Logs do not include this information. A security engineer needs to recommend a solution.

Which combination of steps should the security engineer recommend? (Select TWO )

- A. Edit the existing VPC Flow Log
- B. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
- C. Delete and recreate the existing VPC Flow Log
- D. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
- E. Change the destination to Amazon CloudWatch Logs.
- F. Include the pkt-srcaddr and pkt-dstaddr fields in the log format.
- G. Include the subnet-id and instance-id fields in the log format.

**Answer: AE**

### NEW QUESTION 3

- (Exam Topic 1)

A company uses Microsoft Active Directory for access management for on-premises resources and wants to use the same mechanism for accessing its AWS accounts. Additionally, the development team plans to launch a public-facing application for which they need a separate authentication solution.

When combination of the following would satisfy these requirements? (Select TWO)

- A. Set up domain controllers on Amazon EC2 to extend the on-premises directory to AWS
- B. Establish network connectivity between on-premises and the user's VPC
- C. Use Amazon Cognito user pools for application authentication
- D. Use AD Connector for application authentication.
- E. Set up federated sign-in to AWS through ADFS and SAML.

**Answer: CD**

### NEW QUESTION 4

- (Exam Topic 1)

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

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

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

**Answer: A**

**NEW QUESTION 5**

- (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 6**

- (Exam Topic 1)

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

Which solution will meet this requirement?

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

**Answer: A**

**NEW QUESTION 7**

- (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 8**

- (Exam Topic 1)

A company's Security Officer is concerned about the risk of AWS account root user logins and has assigned a Security Engineer to implement a notification solution for near-real-time alerts upon account root user logins.

How should the Security Engineer meet these requirements?

- A. Create a cron job that runs a script to download the AWS IAM security credentials.
- B. Parse the file for account root user logins and email the Security team's distribution list.
- C. Run AWS CloudTrail logs through Amazon CloudWatch Events to detect account root user logins and trigger an AWS Lambda function to send an Amazon SNS notification to the Security team's distribution list.
- D. Save AWS CloudTrail logs to an Amazon S3 bucket in the Security team's account. Process the CloudTrail logs with the Security Engineer's logging solution for account root user logins. Send an Amazon SNS notification to the Security team upon encountering the account root user login events.
- E. Save VPC Flow Logs to an Amazon S3 bucket in the Security team's account and process the VPC Flow Logs with their logging solutions for account root user logins. Send an Amazon SNS notification to the Security team upon encountering the account root user login events.

**Answer: B**

**NEW QUESTION 9**

- (Exam Topic 1)

A company has decided to use encryption in its AWS account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16,000 B to 5 MB. The requirements are as follows:

- The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
- The key material must be available in multiple Regions. Which option meets these requirements?

- A. Use an AWS KMS customer managed key and store the key material in AWS with replication across Regions.
- B. Use an AWS customer managed key, import the key material into AWS KMS using in-house AWS CloudHSM.
- C. and store the key material securely in Amazon S3.
- D. Use an AWS KMS custom key store backed by AWS CloudHSM clusters, and copy backups across Regions.
- E. Use AWS CloudHSM to generate the key material and backup keys across Regions. Use the Java Cryptography Extension (JCE) and Public Key Cryptography Standards #11 (PKCS #11) encryption libraries to encrypt and decrypt the data.

**Answer: D**

**NEW QUESTION 10**

- (Exam Topic 1)

A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An AWS WAF web ACL is associated with the ALB. AWS CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs. The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked. Which set of actions will identify the suspect attacker's IP address for future occurrences?

- A. Configure VPC Flow Logs on the subnet where the ALB is located, and stream the data CloudWatch. Search for the new-user-creation.php occurrences in CloudWatch.
- B. Configure the CloudWatch agent on the ALB Configure the agent to send application logs to CloudWatch Update the instance role to allow CloudWatch Logs access
- C. Export the logs to CloudWatch Search for the new-user-creation.php occurrences in CloudWatch.
- D. Configure the ALB to export access logs to an Amazon Elasticsearch Service cluster, and use the service to search for the new-user-creation.php occurrences.
- E. Configure the web ACL to send logs to Amazon Kinesis Data Firehose, which delivers the logs to an S3 bucket Use Amazon Athena to query the logs and find the new-user-creation.php occurrences.

**Answer: B**

**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 11**

- (Exam Topic 1)

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

- A. Associate the instances to the same security groups.
- B. Add 0.0.0.0/0 to the egress rules of the instance security groups.
- C. Add the instance IDs to the ingress rules of the instance security groups.
- D. Add the public IP addresses to the ingress rules of the instance security groups.

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-ins>

**NEW QUESTION 14**

- (Exam Topic 1)

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

A

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

B

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

C

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



```
D

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

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

**Answer: A**

#### NEW QUESTION 17

- (Exam Topic 1)

A company has a VPC with an IPv6 address range and a public subnet with an IPv6 address block. The VPC currently hosts some public Amazon EC2 instances but a Security Engineer needs to migrate a second application into the VPC that also requires IPv6 connectivity.

This new application will occasionally make API requests to an external, internet-accessible endpoint to receive updates. However, the Security team does not want the application's EC2 instance exposed directly to the internet. The Security Engineer intends to create a private subnet with a custom route table and to associate the route table with the private subnet.

What else does the Security Engineer need to do to ensure the application will not be exposed directly to the internet, but can still communicate as required?

- A. Launch a NAT instance in the public subnet. Update the custom route table with a new route to the NAT instance.
- B. Remove the internet gateway, and add AWS PrivateLink to the VPC. Then update the custom route table with a new route to AWS PrivateLink.
- C. Add a managed NAT gateway to the VPC. Update the custom route table with a new route to the gateway.
- D. Add an egress-only internet gateway to the VPC.
- E. Update the custom route table with a new route to the gateway.

**Answer: D**

#### NEW QUESTION 22

- (Exam Topic 1)

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

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

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

**Answer: B**

#### NEW QUESTION 25

- (Exam Topic 1)

A company uses SAML federation with AWS Identity and Access Management (IAM) to provide internal users with SSO for their AWS accounts. The company's identity provider certificate was rotated as part of its normal lifecycle. Shortly after, users started receiving the following error when attempting to log in: "Error: Response Signature Invalid (Service: AWSSecuntyTokenService; Status Code: 400; Error Code: InvalidIdentityToken)"  
A security engineer needs to address the immediate issue and ensure that it will not occur again. Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

- A. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
- B. Upload the new metadata file to the new IAM identity provider entity.
- C. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
- D. Generate a new metadata file and upload it to the IAM identity provider entit
- E. Perform automated or manual rotation of the certificate when required.
- F. Download a new copy of the SAML metadata file from the identity provider Upload the new metadata to the IAM identity provider entity configured for the SAML integration in question.
- G. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
- H. Generate a new copy of the metadata file and create a new IAM identity provider entit
- I. Upload the metadata file to the new IAM identity provider entit
- J. Perform automated or manual rotation of the certificate when required.
- K. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
- L. Upload the new metadata file to the new IAM identity provider entit
- M. Update the identity provider configurations to pass a new IAM identity provider entity name in the SAML assertion.

**Answer:** AD

### NEW QUESTION 28

- (Exam Topic 1)

After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from AWS stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.  
How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

- A. Give consent to the AWS Security team to dump the memory core on the compromised instance and provide it to AWS Support for analysis.
- B. Review memory dump data that the AWS Systems Manager Agent sent to Amazon CloudWatch Logs.
- C. Download and run the EC2Rescue for Windows Server utility from AWS.
- D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

**Answer:** B

### NEW QUESTION 30

- (Exam Topic 1)

A company's Security Engineer has been asked to monitor and report all AWS account root user activities. Which of the following would enable the Security Engineer to monitor and report all root user activities?  
(Select TWO)

- A. Configuring AWS Organizations to monitor root user API calls on the paying account
- B. Creating an Amazon CloudWatch Events rule that will trigger when any API call from the root user is reported
- C. Configuring Amazon Inspector to scan the AWS account for any root user activity
- D. Configuring AWS Trusted Advisor to send an email to the Security team when the root user logs in to the console
- E. Using Amazon SNS to notify the target group

**Answer:** BE

### NEW QUESTION 31

- (Exam Topic 1)

A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7 All of the company's AWS applications are serverless with static content hosted on Amazon S3 using Amazon CloudFront and Amazon Route 53  
Which solution will meet these requirements?

- A. Use AWS WAF with an upgrade to the AWS Business support plan
- B. Use AWS Certificate Manager with an Application Load Balancer configured with an origin access identity
- C. Use AWS Shield Advanced
- D. Use AWS WAF to protect AWS Lambda functions encrypted with AWS KMS and a NACL restricting all Ingress traffic

**Answer:** C

### NEW QUESTION 36

- (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 SSLTLS 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 AL
- 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 38**

- (Exam Topic 1)

A company's development team is designing an application using AWS Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company's security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application's AWS services. The solution must minimize management overhead.

How should the security team prevent privilege escalation for both teams?

- A. Enable AWS CloudTrail
- B. Create a Lambda function that monitors the event history for privilege escalation events and notifies the security team.
- C. Create a managed IAM policy for the permissions require
- D. Reference the IAM policy as a permissions boundary within the development team's IAM role.
- E. Enable AWS Organizations Create an SCP that allows the IAM CreateUser action but that has a condition that prevents API calls other than those required by the development team
- F. Create an IAM policy with a deny on the IAMCreateUser action and assign the policy to the development tea
- G. Use a ticket system to allow the developers to request new IAM roles for their application
- H. The IAM roles will then be created by the security team.

**Answer:** A

**NEW QUESTION 43**

- (Exam Topic 1)

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

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

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

**Answer:** CD

**NEW QUESTION 44**

- (Exam Topic 1)

A security engineer need to ensure their company's uses of AWS meets AWS security best practices. As part of this, the AWS account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used. Which solution meets these requirements?

- A. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification.
- B. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification logs from S3 and generate notifications using Amazon SNS.
- C. Set up a rule in AWS config to trigger root user event
- D. Trigger an AWS Lambda function and generate notifications using Amazon SNS.
- E. Use Amazon Inspector to monitor the usage of the root user and generate notifications using Amazon SNS

**Answer:** A

**NEW QUESTION 49**

- (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 of 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 52**

- (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 has a serverless application for internal users deployed on AWS. The application uses AWS Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC. The company uses AWS Systems Manager Parameter Store for storing database credentials. A recent security review highlighted the following issues:

- The Lambda function has internet access.
- The relational database is publicly accessible.
- The database credentials are not stored in an encrypted state.

Which combination of steps should the company take to resolve these security issues? (Select THREE)

- A. Disable public access to the RDS database inside the VPC
- B. Move all the Lambda functions inside the VPC.
- C. Edit the IAM role used by Lambda to restrict internet access.
- D. Create a VPC endpoint for Systems Manager
- E. Store the credentials as a string parameter
- F. Change the parameter type to an advanced parameter.
- G. Edit the IAM role used by RDS to restrict internet access.
- H. Create a VPC endpoint for Systems Manager
- I. Store the credentials as a SecureString parameter.

**Answer:** ABE

#### NEW QUESTION 58

- (Exam Topic 1)

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

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

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

**Answer:** B

#### NEW QUESTION 63

- (Exam Topic 1)

A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the AWS Management Console.

Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?

- A. Enable AWS Systems Manager in the AWS Management Console and configure for access to EC2 instances using the default AmazonEC2RoleforSSM role.
- B. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.
- C. Configure IAM user policies to allow development team access to the Systems Manager Session Manager and attach to the team's IAM users.
- D. Enable console SSH access in the EC2 console.
- E. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the development team's IAM users.
- F. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role.
- G. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.
- H. Configure a security group that allows SSH port 22 from all published IP addresses.
- I. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the team's IAM users.
- J. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access.
- K. Configure IAM policies to allow development team access to the EC2 console and attach to the team's IAM users.

**Answer:** A

#### NEW QUESTION 64

- (Exam Topic 1)

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

What should the Security Engineer do to meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to monitor the AWS CloudTrail configuration.
- B. Send notifications using Amazon SNS.
- C. Create an Amazon CloudWatch Events rule to monitor Amazon GuardDuty findings.
- D. Send email notifications using Amazon SNS.

- E. Update security contact details in AWS account settings for AWS Support to send alerts when suspicious activity is detected.
- F. Use Amazon Inspector to automatically detect security issue
- G. Send alerts using Amazon SNS.

**Answer:** B

#### NEW QUESTION 65

- (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 67

- (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 70

- (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 72

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 75

- (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 78

- (Exam Topic 1)

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

Which of the following actions could fix this issue?

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

**Answer:** C

#### NEW QUESTION 79

- (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 83

- (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 87

- (Exam Topic 2)

A Security Engineer who was reviewing AWS Key Management Service (AWS KMS) key policies found this statement in each key policy in the company AWS account.

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": "kms:*",
  "Resource": "*"
}
```

What does the statement allow?

- A. All principals from all AWS accounts to use the key.
- B. Only the root user from account 111122223333 to use the key.
- C. All principals from account 111122223333 to use the key but only on Amazon S3.
- D. Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

**Answer:** D

#### NEW QUESTION 88

- (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:

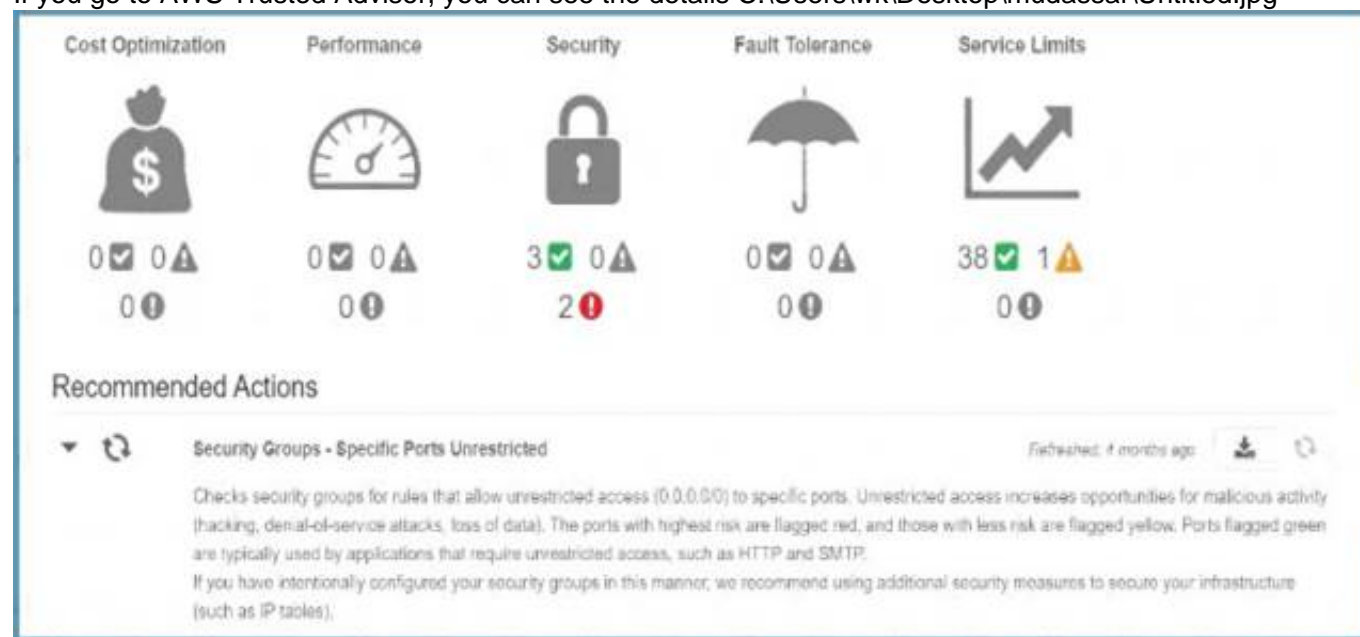
- A. Use AWS Inspector to inspect all the security Groups
- B. Use the AWS Trusted Advisor to see which security groups have compromised access.
- C. Use AWS Config to see which security groups have compromised access.
- D. Use the AWS CLI to query the security groups and then filter for the rules which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

**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 D is 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 91**

- (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 95**

- (Exam Topic 2)

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

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

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

**Answer: AE**

**Explanation:**

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

**NEW QUESTION 96**

- (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": "*"
    }
  ]
}
```

- 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 99**

- (Exam Topic 2)

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

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

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.

What does the Administrator need to change to grant access to the user?

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

**Answer:** A

#### NEW QUESTION 101

- (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 102

- (Exam Topic 2)

A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user’s IAM permissions in the case of a security incident.

How can this be accomplished?

- A. Use AWS Config to review the IAM policy assigned to users before and after the incident.
- B. Run the GenerateCredentialReport via the AWS CLI, and copy the output to Amazon S3 daily for auditing purposes.
- C. Copy AWS CloudFormation templates to S3, and audit for changes from the template.
- D. Use Amazon EC2 Systems Manager to deploy images, and review AWS CloudTrail logs for changes.

**Answer:** A

#### Explanation:

<https://aws.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-aws>

#### NEW QUESTION 104

- (Exam Topic 2)

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

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

- A. Digitized files -> Amazon Kinesis Data Analytics
- B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
- C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
- D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

**Answer:** B

#### NEW QUESTION 109

- (Exam Topic 2)

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

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

Why did GuardDuty fail to alert to this behavior?

- A. GuardDuty did not have the appropriate alerts activated.
- B. GuardDuty does not see these DNS requests.
- C. GuardDuty only monitors active network traffic flow for command-and-control activity.
- D. GuardDuty does not report on command-and-control activity.

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 111

- (Exam Topic 2)

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

- A. Conduct an audit on a yearly basis
- B. Conduct an audit if application instances have been added to your account
- C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
- D. Whenever there are changes in your organization

**Answer:** A

**Explanation:**

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

You should audit your security configuration in the following situations: On a periodic basis.

If there are changes in your organization, such as people leaving.

If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need.

If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWorks stacks, AWS CloudFormation templates, etc.

If you ever suspect that an unauthorized person might have accessed your account.

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

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

The correct answer is: Conduct an audit on a yearly basis Submit your Feedback/Queries to our Experts

**NEW QUESTION 116**

- (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 118**

- (Exam Topic 2)

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

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

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

**Answer:** C

**NEW QUESTION 122**

- (Exam Topic 2)

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

- A. AWS CloudTrail
- B. Amazon Athena
- C. AWS Key Management Service (AWS KMS)
- D. VPC Flow Logs
- E. AWS Firewall Manager
- F. Security groups

**Answer:** ADF

**Explanation:**

[https://github.com/awslabs/aws-well-architected-labs/blob/master/Security/300\\_Incident\\_Response\\_with\\_AWS](https://github.com/awslabs/aws-well-architected-labs/blob/master/Security/300_Incident_Response_with_AWS)

**NEW QUESTION 126**

- (Exam Topic 2)

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

- A. Use the AWS account root user access keys instead of the AWS Management Console
- B. Enable multi-factor authentication for the AWS IAM users with the AdministratorAccess managed policy attached to them
- C. Enable multi-factor authentication for the AWS account root user
- D. Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days



E. Do not create access keys for the AWS account root user; instead, create AWS IAM users

**Answer:** CE

#### NEW QUESTION 129

- (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 133

- (Exam Topic 2)

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

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

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

**Answer:** BE

#### NEW QUESTION 135

- (Exam Topic 2)

A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.

Which solution would be MOST secure and easy to maintain?

- A. Use AWS Certificate Manager to generate certificates from a public certificate authority and deploy them to all the containers.
- B. Create a self-signed certificate in one container and use AWS Secrets Manager to distribute the certificate to the other containers to establish trust.
- C. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then create the private keys in the containers and sign them using the ACM PCA API.
- D. Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then use AWS Certificate Manager to generate the private certificates and deploy them to all the containers.

**Answer:** D

#### NEW QUESTION 136

- (Exam Topic 2)

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

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

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

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

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

**Answer:** AB

#### NEW QUESTION 141

- (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 145

- (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 147

- (Exam Topic 2)

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

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

- A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
- B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
- C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
- D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
- E. Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

**Answer: AB**

#### Explanation:

[https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6\\_NybQPhh6tRP/Cloudwatch%](https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%20logs%20stop%20being%20delivered%20after%20a%20specific%20number%20of%20hours)

**NEW QUESTION 151**

- (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 152**

- (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 154**

- (Exam Topic 2)

The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.

Pattern: "randomID\_datestamp\_PII.csv" Example:

"1234567\_12302017\_000-00-0000.csv"

The bucket where these objects are being stored is using server-side encryption (SSE). Which solution is the most secure and cost-effective option to protect the sensitive data?

- A. Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.
- B. Add an S3 bucket policy that denies the action s3:GetObject.
- C. Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.
- D. Store all sensitive objects in Binary Large Objects (BLOBs) in an encrypted Amazon RDS instance.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html> <https://aws.amazon.com/blogs/database/best-practices-for-securing-sensitive-data-in-aws-data-stores/>

**NEW QUESTION 157**

- (Exam Topic 2)

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

How can this be accomplished? (Choose two.)



- A. Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPCs.
- B. Do not complete the penetration test request form.

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

**Answer:** BD

**Explanation:**

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

**NEW QUESTION 162**

- (Exam Topic 2)

An organization has three applications running on AWS, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an AWS KMS Customer Master Key (CMK).

What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

- A. Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.
- B. Have each application assume an IAM role that provides permissions to use the AWS Certificate Manager CMK.
- C. Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.
- D. Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.

**Answer:** C

**NEW QUESTION 166**

- (Exam Topic 2)

A Developer who is following AWS best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using AWS KMS. What is the simplest and MOST secure way to decrypt this data when required?

- A. Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.
- B. Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policie
- C. Query DynamoDB to retrieve the data key to decrypt the data
- D. Use the Encrypt API to store an encrypted version of the data key with another customer managed key. Decrypt the data key and use it to decrypt the data when required.
- E. Store the encrypted data key alongside the encrypted dat
- F. Use the Decrypt API to retrieve the data key to decrypt the data when required.

**Answer:** D

**Explanation:**

We recommend that you use the following pattern to locally encrypt data: call the GenerateDataKey API, use the key returned in the Plaintext response field to locally encrypt data, and then erase the plaintext data key from memory. Store the encrypted data key (contained in the CiphertextBlob field) alongside of the locally encrypted data. The Decrypt API returns the plaintext key from the encrypted key.

<https://docs.aws.amazon.com/sdkfornet/latest/apidocs/items/MKeyManagementServiceKeyManagementService>

**NEW QUESTION 169**

- (Exam Topic 2)

You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?

Please select:

- A. Use versioning and enable a timestamp for each version
- B. Use Pre-signed URL's
- C. Use IAM Roles with a timestamp to limit the access
- D. Use IAM policies with a timestamp to limit the access

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.

Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:

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

The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

**NEW QUESTION 173**

- (Exam Topic 2)

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

Which of the following troubleshooting steps should the Analyst perform?



- A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's AWS account
- B. Verify that a metric filter was created and then mapped to an alarm
- C. Check the alarm notification action.
- D. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
- E. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

**Answer:** B

**Explanation:**

MetricFilter:

Type: 'AWS::Logs::MetricFilter' Properties:

LogGroupName: " FilterPattern: >

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||  
($.eventName = RevokeSecurityGroupEgress)  
|| ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }
```

MetricTransformations:

- MetricValue: '1'

MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

**NEW QUESTION 174**

- (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 176**

- (Exam Topic 2)

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Please select:

- A. Enable MFA for these user accounts
- B. Enable versioning for these user accounts
- C. Enable accidental deletion for these user accounts
- D. Disable root access for the users

**Answer:** A

**Explanation:**

The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Option B,C and D are invalid because no such security options are available in AWS For more information on IAM best practices, please visit the below URL

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The correct answer is: Enable MFA for these user accounts

Submit your Feedback/Queries to our Experts

**NEW QUESTION 181**

- (Exam Topic 2)

You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?

Please select:

- A. Shutdown the instance
- B. Remove the rule for incoming traffic on port 22 for the Security Group
- C. Change the AMI for the instance
- D. Change the Instance type for the instance

**Answer:** B

**Explanation:**

In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.

Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.

For more information on authorizing access to an instance, please visit the below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

**NEW QUESTION 186**

- (Exam Topic 2)

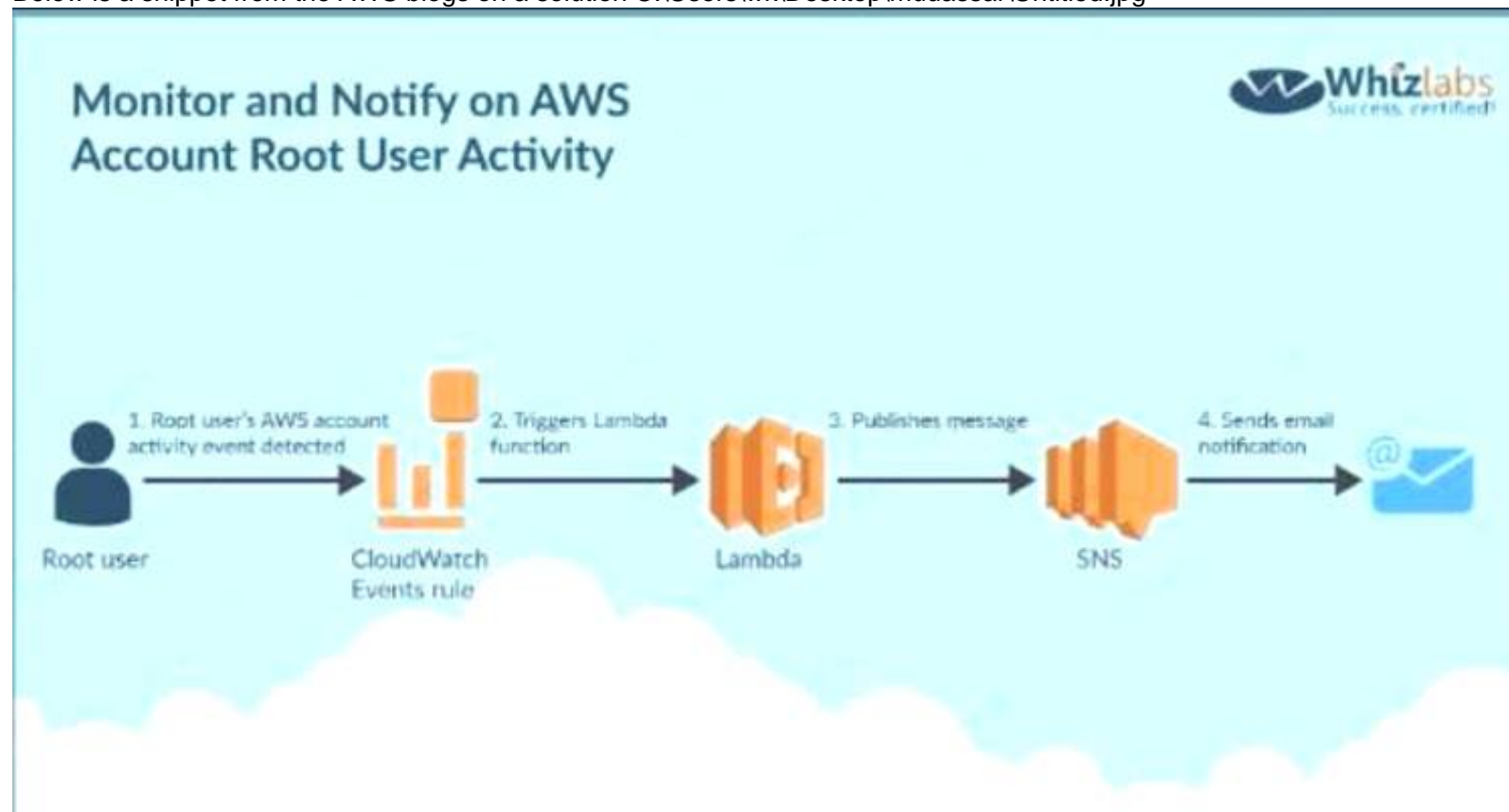
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution  
Please select:

- A. Create a Cloudwatch Events Rule s
- B. Create a Cloudwatch Logs Rule
- C. Use a Lambda function
- D. Use Cloudtrail API call

**Answer:** AC

**Explanation:**

Below is a snippet from the AWS blogs on a solution C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL: <https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity> The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts

**NEW QUESTION 190**

- (Exam Topic 2)

You have enabled Cloudtrail logs for your company's AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?  
Please select:

- A. Enable SSL certificates for the Cloudtrail logs
- B. There is no need to do anything since the logs will already be encrypted
- C. Enable Server side encryption for the trail
- D. Enable Server side encryption for the destination S3 bucket

**Answer:** B

**Explanation:**

The AWS Documentation mentions the following.

By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.

Option A.C and D are not valid since logs will already be encrypted

For more information on how Cloudtrail works, please visit the following URL: <https://docs.aws.amazon.com/awscloudtrail/latest/useruide/how-cloudtrail-works.html>

The correct answer is: There is no need to do anything since the logs will already be encrypted Submit your Feedback/Queries to our Experts

**NEW QUESTION 195**

- (Exam Topic 2)

You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.  
Please select:

- A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0
- B. db-345 - Allow port 1433 from wg-123
- C. wg-123 - Allow port 1433 from wg-123
- D. db-345 -Allow ports 1433 from 0.0.0.0/0

**Answer:** AB

**Explanation:**

The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.

The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration

Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123

Submit your Feedback/Queries to our Experts

**NEW QUESTION 197**

- (Exam Topic 2)

An organization is moving non-business-critical applications to AWS while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in AWS. The internet performance is unpredictable.

Which configuration will ensure continued connectivity between sites MOST securely?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 199**

- (Exam Topic 2)

An Amazon EC2 instance is denied access to a newly created AWS KMS CMK used for decrypt actions. The environment has the following configuration:

- The instance is allowed the kms:Decrypt action in its IAM role for all resources
  - The AWS KMS CMK status is set to enabled
  - The instance can communicate with the KMS API using a configured VPC endpoint
- What is causing the issue?

- A. The kms:GenerateDataKey permission is missing from the EC2 instance's IAM role
- B. The ARN tag on the CMK contains the EC2 instance's ID instead of the instance's ARN
- C. The kms:Encrypt permission is missing from the EC2 IAM role
- D. The KMS CMK key policy that enables IAM user permissions is missing

**Answer:** A

**Explanation:**

In a key policy, you use "\*" for the resource, which means "this CMK." A key policy applies only to the CMK it is attached to

References:

**NEW QUESTION 201**

- (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 205**

- (Exam Topic 2)

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

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 208**

- (Exam Topic 2)

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

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

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

**Answer:** CDE

**NEW QUESTION 210**

- (Exam Topic 2)

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

- A. The external ID used by the Auditor is missing or incorrect.
- B. The Auditor is using the incorrect password.
- C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.
- D. The Amazon EC2 role used by the Auditor must be set to the destination account role.
- E. The secret key used by the Auditor is missing or incorrect.
- F. The role ARN used by the Auditor is missing or incorrect.

**Answer:** ACF

**Explanation:**

Using IAM to grant access to a Third-Party Account 1) Create a role to provide access to the require resources 1.1) Create a role policy that specifies the AWS Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition 1.2) Create a role using the role policy just created 1.3) Assign a resouce policy to the role. This will provide permission to access resource ARNs to the auditor 2) Repeat steps 1 and 2 on all AWS accounts 3) The auditor connects to the AWS account AWS Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3, sts:ExternalID 4) STS provide the auditor with temporary credentials that provides the role access from step 1

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_create\\_for-user\\_externalid.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html)

<https://aws.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-aws-cloudtrail-and-amazon-clou>

**NEW QUESTION 214**

- (Exam Topic 2)

An application uses Amazon Cognito to manage end users' permissions when directly accessing AWS resources, including Amazon DynamoDB. A new feature request reads as follows:

Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.

The priorities are to reduce complexity and avoid potential for future security issues. Which approach will meet these requirements and priorities?

- A. Create a new database field "suspended\_status" and modify the application logic to validate that field when processing requests.
- B. Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.
- C. Use Amazon Cognito Sync to push out a "suspension\_status" parameter and split the IAM policy into normal users and suspended users.
- D. Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

**Answer:** D

**Explanation:**

<https://aws.amazon.com/blogs/aws/new-amazon-cognito-groups-and-fine-grained-role-based-access-control-2/>

**NEW QUESTION 217**

- (Exam Topic 2)

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

What is the MOST efficient way to meet these requirements?

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

**Answer:** B

**NEW QUESTION 220**



- (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 225**

- (Exam Topic 2)

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

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

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

**Answer: AD**

**NEW QUESTION 228**

- (Exam Topic 3)

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

Please select:

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

**Answer: A**

**Explanation:**

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

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

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

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

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

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

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

Submit your Feedback/Queries to our Experts

**NEW QUESTION 229**

- (Exam Topic 3)

There is a set of EC2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?

Please select:

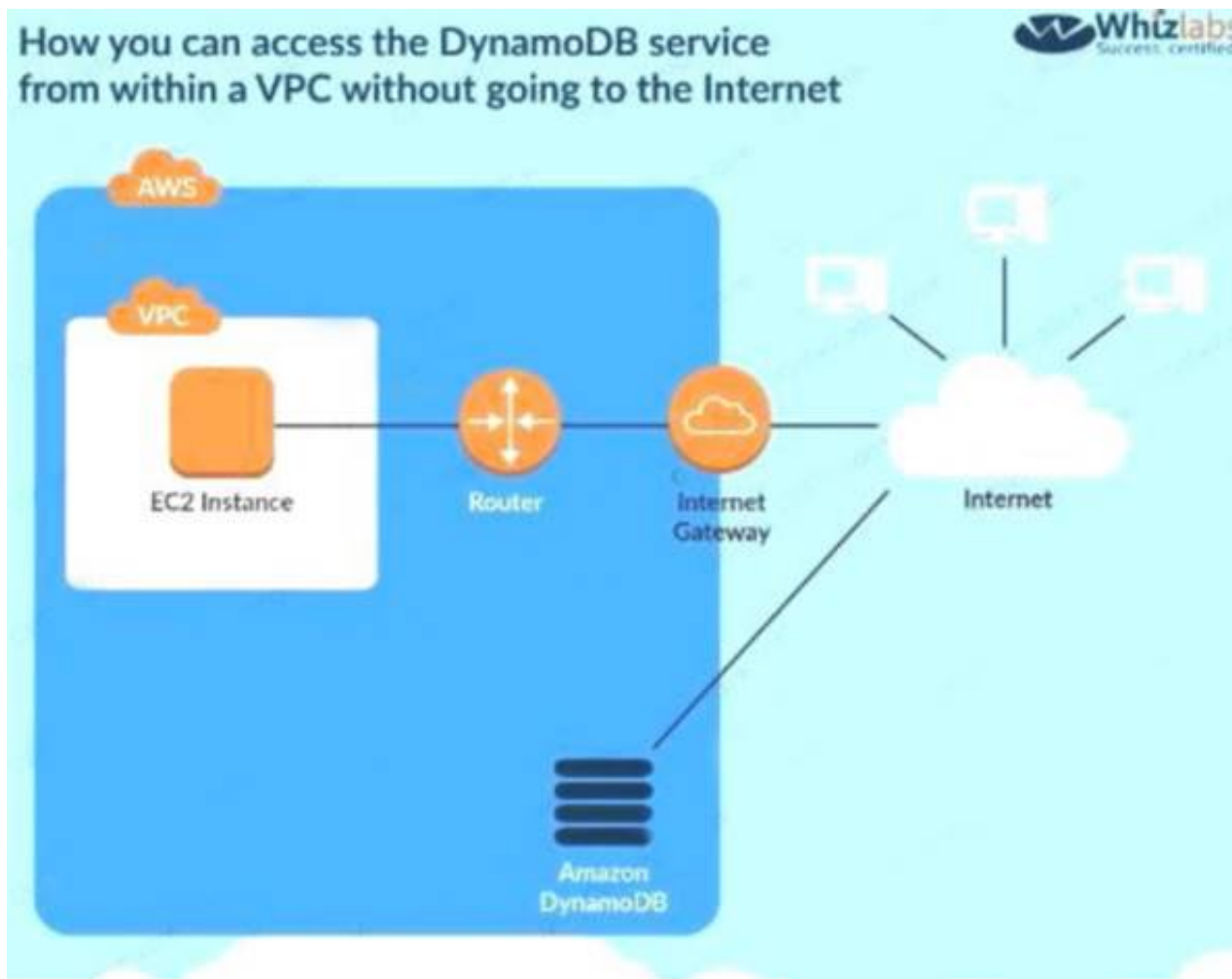
- A. Use a VPC endpoint to the DynamoDB table
- B. Use a VPN connection from the VPC
- C. Use a VPC gateway from the VPC
- D. Use a VPC Peering connection to the DynamoDB table

**Answer: A**

**Explanation:**

The following diagram from the AWS Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be done with the help of a VPC endpoint

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



Option B is invalid because this is used for connection between an on-premise solution and AWS Option C is invalid because there is no such option

Option D is invalid because this is used to connect 2 VPCs

For more information on VPC endpoints for DynamoDB, please visit the URL:

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

#### NEW QUESTION 231

- (Exam Topic 3)

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

Please select:

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

**Answer: B**

#### Explanation:

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

Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that IAM users and groups are created For more information on the Systems Manager role please refer to the below URL: [com/systems-manageer/latest/useruide/sysman-!](https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-!)

The correct answer is: Ensure that an IAM service role is created Submit your Feedback/Queries to our Experts

#### NEW QUESTION 236

- (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 followi .

- 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 239

- (Exam Topic 3)

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

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

**Answer: C**

#### Explanation:

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

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

Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originate', from the IT admin's workstation. The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

#### NEW QUESTION 242

- (Exam Topic 3)

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

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

Please select:

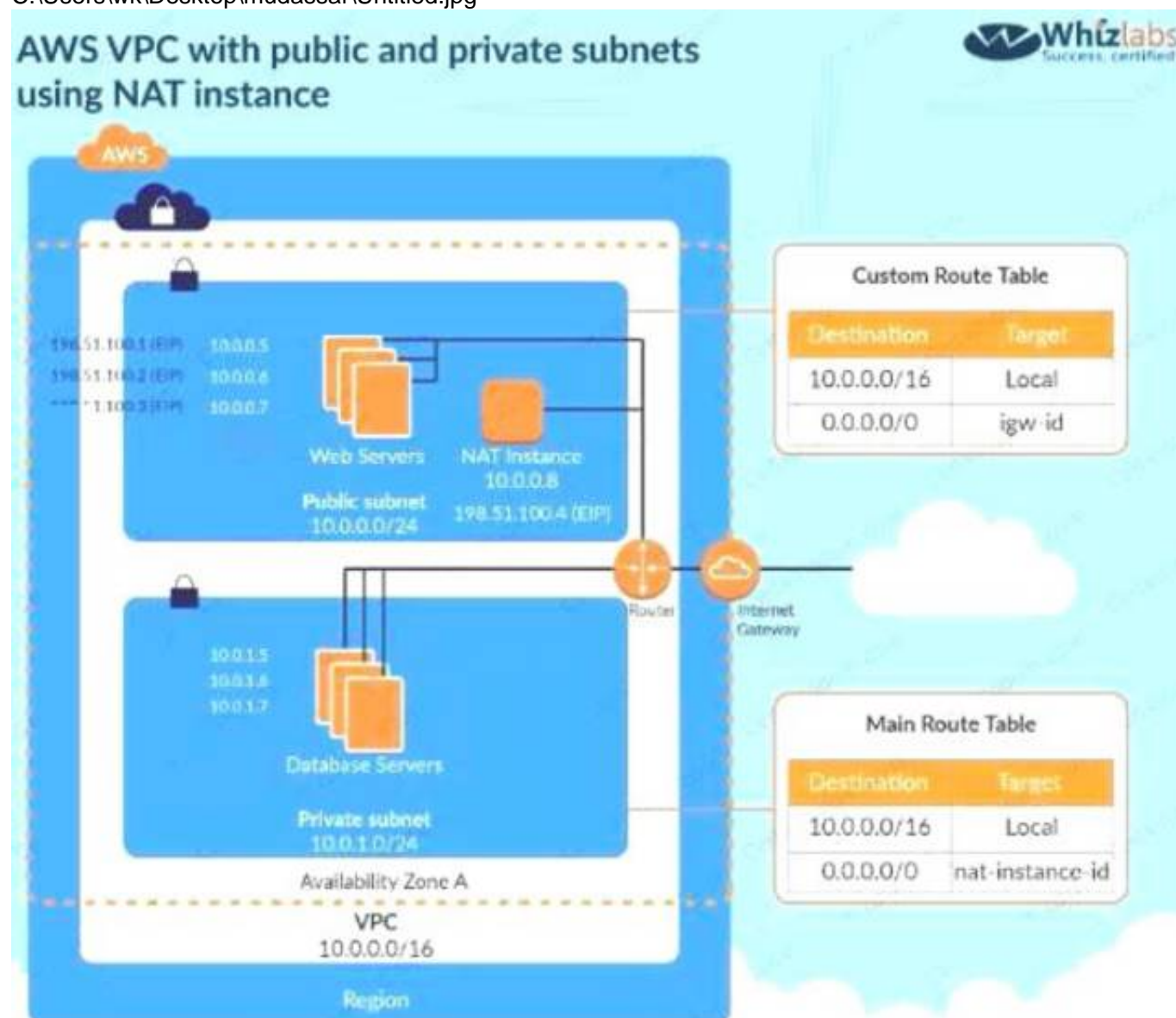
- A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
- B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
- C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
- D. EC2 instances in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

**Answer: D**

#### Explanation:

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

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



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

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

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

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

#### NEW QUESTION 243

- (Exam Topic 3)



You have an S3 bucket defined in AWS. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this. Please select:

- A. Enable server side encryption for the S3 bucket
- B. This request will ensure that the data is encrypted first.
- C. Use the AWS Encryption CLI to encrypt the data first
- D. Use a Lambda function to encrypt the data before sending it to the S3 bucket.
- E. Enable client encryption for the bucket

**Answer: B**

**Explanation:**

One can use the AWS Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL:

<https://aws.amazon.com/blogs/security/how-to-encrypt-and-decrypt-your-data-with-the-aws-encryption-cli/>

The correct answer is: Use the AWS Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

**NEW QUESTION 248**

- (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-signers.html> The correct answer is: Create pre-signed URL's Submit your Feedback/Queries to our Experts

**NEW QUESTION 252**

- (Exam Topic 3)

A company is running an application in The eu-west-1 Region. The application uses an AWS Key Management Service (AWS KMS) CMK to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region.

A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code.

Which change should the security engineer make to the AWS KMS configuration to meet these requirements?

- A. Update the key policies in eu-west-1. Point the application in eu-north-1 to use the same CMK as the application in eu-west-1.
- B. Allocate a new CMK to eu-north-1 to be used by the application that is deployed in that Region.
- C. Allocate a new CMK to eu-north-1. Create the same alias name for both key
- D. Configure the application deployment to use the key alias.
- E. Allocate a new CMK to eu-north-1. Create an alias for eu-north-1. Change the application code to point to the alias for eu-north-1.

**Answer: B**

**NEW QUESTION 253**

- (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 255

- (Exam Topic 3)

A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.

Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

- A. Create an AWS Config rule to detect the creation of unencrypted RDS database
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger on the AWS Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- C. Use AWS System Manager State Manager to detect RDS database encryption configuration drift
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- E. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the process
- F. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.
- G. Take a snapshot of the unencrypted RDS database
- H. Copy the snapshot and enable snapshot encryption in the process
- I. Restore the database instance from the newly created encrypted snapshot
- J. Terminate the unencrypted database instance.
- K. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database

**Answer: AD**

#### NEW QUESTION 256

- (Exam Topic 3)

A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private. How can this be ensured continually?

Choose 2 answers from the options given below

Please select:

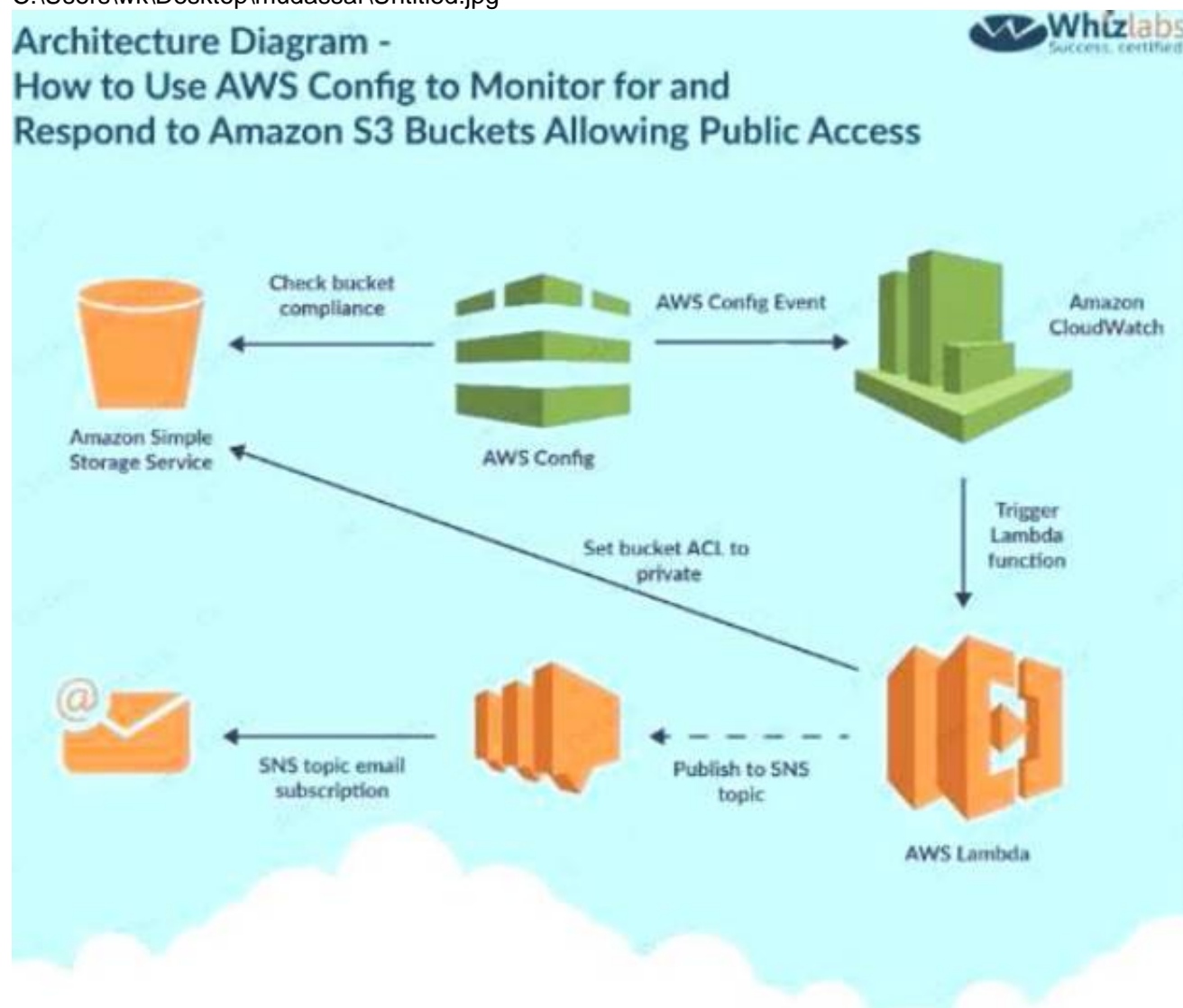
- A. Use AWS Config to monitor changes to the AWS Bucket
- B. Use AWS Lambda function to change the bucket policy
- C. Use AWS Trusted Advisor API to monitor the changes to the AWS Bucket
- D. Use AWS Lambda function to change the bucket ACL

**Answer: AD**

#### Explanation:

One of the AWS Blogs mentions the usage of AWS Config and Lambda to achieve this. Below is the diagram representation of this

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



Option C is invalid because the Trusted Advisor API cannot be used to monitor changes to the AWS Bucket. Option B doesn't seem to be the most appropriate.

\* 1. If the object is in a bucket in which all the objects need to be private and the object is not private anymore, the Lambda function makes a PutObjectAcl call to S3 to make the object private.  
|<https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-a> The following link also specifies that Create a new Lambda function to examine an Amazon S3 buckets ACL and bucket policy. If the bucket ACL is found to al public access, the Lambda function overwrites it to be private. If a bucket policy is found, the Lambda function creatt an SNS message, puts the policy in the message body, and publishes it to the Amazon SNS topic we created. Bucket policies can be complex, and overwriting your policy may cause unexpected loss of access, so this Lambda function doesn't attempt to alter your policy in any way.  
<https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucke> Based on these facts Option D seems to be more appropriate then Option B.  
For more information on implementation of this use case, please refer to the Link: <https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucke>  
The correct answers are: Use AWS Config to monitor changes to the AWS Bucket Use AWS Lambda function to change the bucket ACL

**NEW QUESTION 259**

- (Exam Topic 3)

How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance. How can this be achieved?  
Please select:

- A. Change the existing DHCP options set
- B. Create a new DHCP options set and replace the existing one.
- C. Change the route table for the VPC
- D. Change the subnet configuration to allow DNS requests from the new DNS Server

**Answer:** B

**Explanation:**

In order to use your own DNS server, you need to ensure that you create a new custom DHCP options set with the IP of th custom DNS server. You cannot modify the existing set, so you need to create a new one.

Option A is invalid because you cannot make changes to an existing DHCP options Set.

Option C is invalid because this can only be used to work with Routes and not with a custom DNS solution. Option D is invalid because this needs to be done at the VPC level and not at the Subnet level

For more information on DHCP options set, please visit the following url [https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC DHCP Options.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC%20DHCP%20Options.html)

The correct answer is: Create a new DHCP options set and replace the existing one. Submit your Feedback/Queries to our Experts

**NEW QUESTION 264**

- (Exam Topic 3)

You work at a company that makes use of AWS resources. One of the key security policies is to ensure that all data i encrypted both at rest and in transit. Which of the following is one of the right ways to implement this.

Please select:

- A. Use S3 SSE and use SSL for data in transit
- B. SSL termination on the ELB
- C. Enabling Proxy Protocol
- D. Enabling sticky sessions on your load balancer

**Answer:** A

**Explanation:**

By disabling SSL termination, you are leaving an unsecure connection from the ELB to the back end instances. Hence this means that part of the data transit is not being encrypted.

Option B is incorrect because this would not guarantee complete encryption of data in transit Option C and D are incorrect because these would not guarantee encryption

For more information on SSL Listeners for your load balancer, please visit the below URL: <http://docs.aws.amazon.com/elasticloadbalancine/latest/classic/elb-https-load-balancers.html> The correct answer is: Use S3 SSE and use SSL for data in transit

Submit your Feedback/Queries to our Experts

**NEW QUESTION 269**

- (Exam Topic 3)

You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets. Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below

Please select:

- A. IAM policies
- B. Buckets ACL's
- C. IAM users
- D. Bucket policies

**Answer:** BD

**Explanation:**

The AWS Security whitepaper gives the type of access control and to what level the control can be given C:\Users\wk\Desktop\mudassar\Untitled.jpg

Type of Access Control	AWS Account-Level Control?	User-Level Control?
IAM Policies	No	Yes
ACLs	Yes	No
Bucket Policies	Yes	Yes

Options A and C are incorrect since for external access to buckets, you need to use either Bucket policies or Bucket ACL's or more information on Security for storage services role please refer to the below URL:

[https://d1.awsstatic.com/whitepapers/Security/Security Storage Services Whitepaper.pdf](https://d1.awsstatic.com/whitepapers/Security/Security%20Storage%20Services%20Whitepaper.pdf) The correct answers are: Buckets ACL's, Bucket policies

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 271

- (Exam Topic 3)

A company's on-premises networks are connected to VPCs using an AWS Direct Connect gateway. The company's on-premises application needs to stream data using an existing Amazon Kinesis Data Firehose delivery stream. The company's security policy requires that data be encrypted in transit using a private network. How should the company meet these requirements?

- A. Create a VPC endpoint for Kinesis Data Firehose
- B. Configure the application to connect to the VPC endpoint.
- C. Configure an IAM policy to restrict access to Kinesis Data Firehose using a source IP condition. Configure the application to connect to the existing Firehose delivery stream.
- D. Create a new TLS certificate in AWS Certificate Manager (ACM). Create a public-facing Network Load Balancer (NLB) and select the newly created TLS certificate
- E. Configure the NLB to forward all traffic to Kinesis Data Firehose
- F. Configure the application to connect to the NLB.
- G. Peer the on-premises network with the Kinesis Data Firehose VPC using Direct Connect
- H. Configure the application to connect to the existing Firehose delivery stream.

**Answer: A**

#### NEW QUESTION 273

- (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 276

- (Exam Topic 3)

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances.

Which of the following would be an effective way to achieve this?

Please select:

- A. Use the AWS Systems Manager Parameter Store
- B. Use the AWS Systems Manager Run Command
- C. Use the AWS Inspector
- D. Use AWS Config

**Answer: B**

#### Explanation:

The AWS Documentation mentions the following

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

Option A is invalid because this service is used to store parameter. Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.

Option D is invalid because this service is used to check for configuration changes. For more information on executing remote commands, please visit the below URL

<https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html>

The correct answer is: Use the AWS Systems Manager Run Command. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 279

- (Exam Topic 3)

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following



Whether any ports are left open other than admin ones like SSH and RDP

Whether any ports to the database server other than ones from the web server security group are open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?

Please select:

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

**Answer: B**

**Explanation:**

Trusted Advisor checks for compliance with the following security recommendations:

Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNC).

Limited access to common database ports. This includes ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).

Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all o these checks on its dashboard

Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in th.

assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2 instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and configuration data (telemetry), which it then passes to the Amazon Inspector service.

Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this question.

Options D is invalid because this service dont provide these details.

For more information on the Trusted Advisor, please visit the following URL <https://aws.amazon.com/premiumsupport/trustedadvisor>

The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

**NEW QUESTION 283**

- (Exam Topic 3)

You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet. This instance needs to connect to an EC2 Instance that will host an Oracle database. Which of the following steps should be followed to ensure a secure setup is in place? Select 2 answers.

Please select:

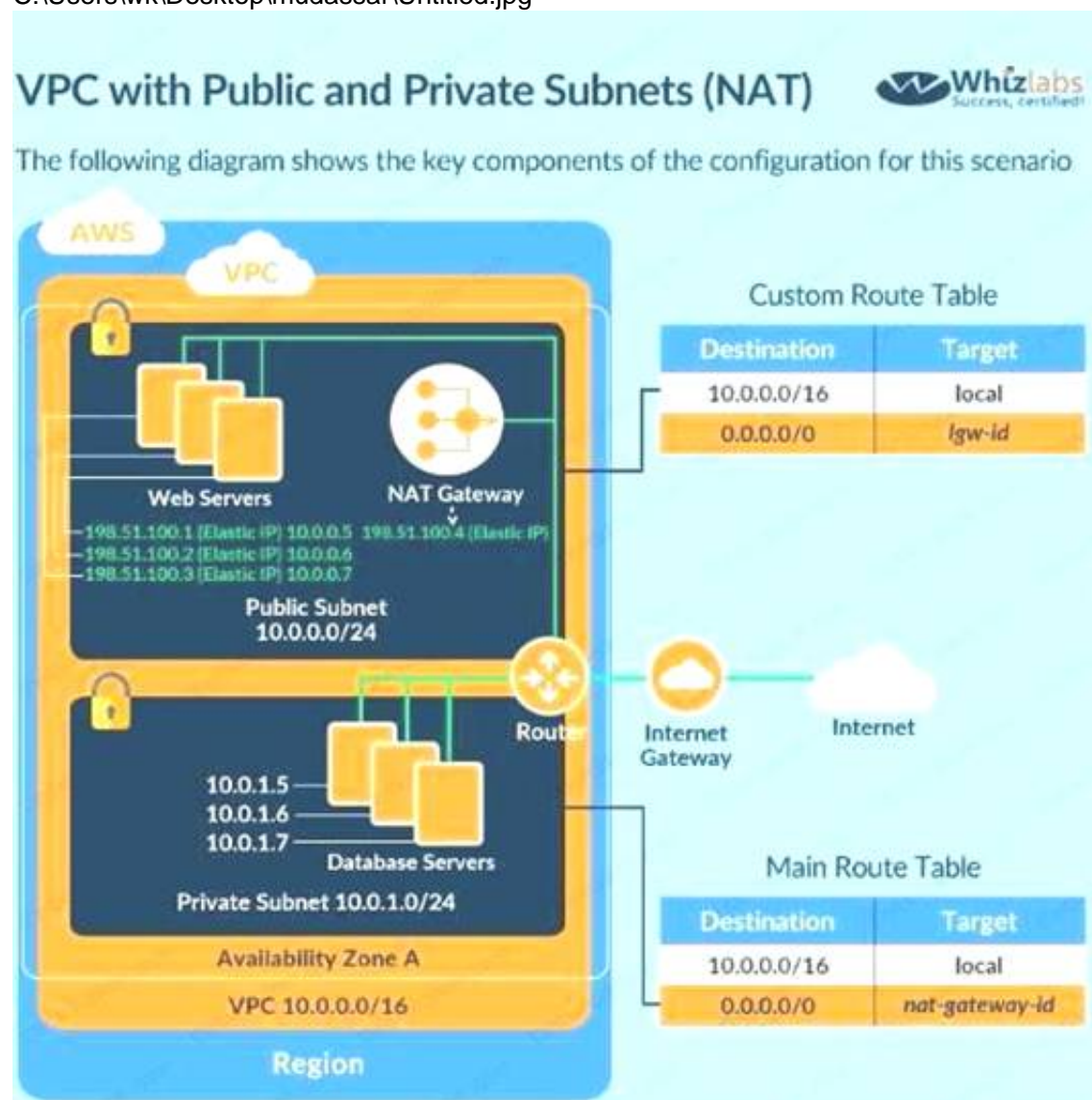
- A. Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication
- B. Place the EC2 Instance with the Oracle database in a separate private subnet
- C. Create a database security group and ensure the web security group to allowed incoming access
- D. Ensure the database security group allows incoming traffic from 0.0.0.0/0

**Answer: BC**

**Explanation:**

The best secure option is to place the database in a private subnet. The below diagram from the AWS Documentation shows this setup. Also ensure that access is not allowed from all sources but just from the web servers.

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



Option A is invalid because databases should not be placed in the public subnet

Option D is invalid because the database security group should not allow traffic from the internet For more information on this type of setup, please refer to the below URL:

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC\\_Scenario2](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_Scenario2).

The correct answers are: Place the EC2 Instance with the Oracle database in a separate private subnet Create a database security group and ensure the web security group to allowed incoming access



Submit your Feedback/Queries to our Experts

**NEW QUESTION 285**

- (Exam Topic 3)

A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?

Please select:

- A. Use Bucket policies
- B. Use the Secure Token service
- C. Use IAM user policies
- D. Use AWS Access Keys

**Answer:** AC

**Explanation:**

The AWS Documentation mentions the following

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below

Link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

**NEW QUESTION 289**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SCS-C01 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SCS-C01-dumps.html>