



# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty

#### NEW QUESTION 1

A company in France uses Amazon Cognito with the Cognito Hosted UI as an identity broker for sign-in and sign-up processes. The company is marketing an application and expects that all the application's users will come from France. When the company launches the application the company's security team observes fraudulent sign-ups for the application. Most of the fraudulent registrations are from users outside of France. The security team needs a solution to perform custom validation at sign-up Based on the results of the validation the solution must accept or deny the registration request. Which combination of steps will meet these requirements? (Select TWO.)

- A. Create a pre sign-up AWS Lambda trigger
- B. Associate the Amazon Cognito function with the Amazon Cognito user pool.
- C. Use a geographic match rule statement to configure an AWS WAF web ACL
- D. Associate the web ACL with the Amazon Cognito user pool.
- E. Configure an app client for the application's Amazon Cognito user pool
- F. Use the app client ID to validate the requests in the hosted UI.
- G. Update the application's Amazon Cognito user pool to configure a geographic restriction setting.
- H. Use Amazon Cognito to configure a social identity provider (IdP) to validate the requests on the hosted UI.

**Answer:** B

#### Explanation:

<https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-lambda-post-authentication.html>

#### NEW QUESTION 2

Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement. Please select:

- A. Set up VPC peering between the central server VPC and each of the teams VPCs.
- B. Set up IAM DirectConnect between the central server VPC and each of the teams VPCs.
- C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.
- D. None of the above options will work.

**Answer:** A

#### Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another IAM account within a single region.

Options B and C are invalid because you need to use VPC Peering Option D is invalid because VPC Peering is available

For more information on VPC Peering please see the below Link:

<http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>

The correct answer is: Set up VPC peering between the central server VPC and each of the teams VPCs. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 3

A company developed an application by using AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS), and Amazon DynamoDB. An external application puts objects into the company's S3 bucket and tags the objects with date and time. A Lambda function periodically pulls data from the company's S3 bucket based on date and time tags and inserts specific values into a DynamoDB table for further processing. The data includes personally identifiable information (PII). The company must remove data that is older than 30 days from the S3 bucket and the DynamoDB table. Which solution will meet this requirement with the MOST operational efficiency?

- A. Update the Lambda function to add a TTL S3 flag to S3 object
- B. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using the TTL S3 flag.
- C. Create an S3 Lifecycle policy to expire objects that are older than 30 day
- D. Update the Lambda function to add the TTL attribute in the DynamoDB table
- E. Enable TTL on the DynamoDB table to expire entries that are older than 30 days based on the TTL attribute.
- F. Create an S3 Lifecycle policy to expire objects that are older than 30 days and to add all prefixes to the S3 bucket
- G. Update the Lambda function to delete entries that are older than 30 days.
- H. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using object tag
- I. Update the Lambda function to delete entries that are older than 30 days.

**Answer:** B

#### NEW QUESTION 4

A company is using an AWS Key Management Service (AWS KMS) AWS owned key in its application to encrypt files in an AWS account The company's security team wants the ability to change to new key material for new files whenever a potential key breach occurs A security engineer must implement a solution that gives the security team the ability to change the key whenever the team wants to do so Which solution will meet these requirements?

- A. Create a new customer managed key Add a key rotation schedule to the key Invoke the key rotation schedule every time the security team requests a key change
- B. Create a new AWS managed key Add a key rotation schedule to the key Invoke the key rotation schedule every time the security team requests a key change
- C. Create a key alias Create a new customer managed key every time the security team requests a key change Associate the alias with the new key
- D. Create a key alias Create a new AWS managed key every time the security team requests a key change Associate the alias with the new key

**Answer:** A

#### Explanation:

To meet the requirement of changing the key material for new files whenever a potential key breach occurs, the most appropriate solution would be to create a new customer managed key, add a key rotation schedule to the key, and invoke the key rotation schedule every time the security team requests a key change.  
References: : Rotating AWS KMS keys - AWS Key Management Service

#### NEW QUESTION 5

A company plans to use AWS Key Management Service (AWS KMS) to implement an encryption strategy to protect data at rest. The company requires client-side encryption for company projects. The company is currently conducting multiple projects to test the company's use of AWS KMS. These tests have led to a sudden increase in the company's AWS resource consumption. The test projects include applications that issue multiple requests each second to KMS endpoints for encryption activities.

The company needs to develop a solution that does not throttle the company's ability to use AWS KMS. The solution must improve key usage for client-side encryption and must be cost optimized. Which solution will meet these requirements?

- A. Use keyrings with the AWS Encryption SD
- B. Use each keyring individually or combine keyrings into a multi-keyrin
- C. Decrypt the data by using a keyring that has the primary key in the multi-keyring.
- D. Use data key cachin
- E. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.
- F. Use KMS key rotatio
- G. Use a local cache in the AWS Encryption SDK with a caching cryptographic materials manager.
- H. Use keyrings with the AWS Encryption SD
- I. Use each keyring individually or combine keyrings into a multi-keyrin
- J. Use any of the wrapping keys in the multi-keyring to decrypt the data.

**Answer: B**

#### Explanation:

The correct answer is B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager. This answer is correct because data key caching can improve performance, reduce cost, and help the company stay within the service limits of AWS KMS. Data key caching stores data keys and related cryptographic material in a cache, and reuses them for encryption and decryption operations. This reduces the number of requests to AWS KMS endpoints and avoids throttling. The AWS Encryption SDK provides a local cache and a caching cryptographic materials manager (caching CMM) that interacts with the cache and enforces security thresholds that the company can set<sup>1</sup>.

The other options are incorrect because:

- A. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization. Keyrings are used to generate, encrypt, and decrypt data keys, but they do not cache or reuse them. Using each keyring individually or combining them into a multi-keyring does not reduce the number of requests to AWS KMS endpoints<sup>2</sup>.
- C. Using KMS key rotation does not address the problem of throttling or cost optimization. Key rotation is a security practice that creates new cryptographic material for a KMS key every year, but it does not affect the data that the KMS key protects. Key rotation does not reduce the number of requests to AWS KMS endpoints, and it might incur additional costs for storing multiple versions of key material<sup>3</sup>.
- D. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization, as explained in option A. Moreover, using any of the wrapping keys in the multi-keyring to decrypt the data is not a valid option, because only one of the wrapping keys can decrypt a given data key. The wrapping key that encrypts a data key is stored in the encrypted data key structure, and only that wrapping key can decrypt it<sup>4</sup>.

References:

1: Data key caching - AWS Encryption SDK 2: Using keyrings - AWS Encryption SDK 3: Rotating AWS KMS keys - AWS Key Management Service 4: How keyrings work - AWS Encryption SDK

#### NEW QUESTION 6

A web application gives users the ability to log in verify their membership's validity and browse artifacts that are stored in an Amazon S3 bucket. When a user attempts to download an object, the application must verify the permission to access the object and allow the user to download the object from a custom domain name such as example.com.

What is the MOST secure way for a security engineer to implement this functionality?

- A. Configure read-only access to the object by using a bucket AC
- B. Remove the access after a set time has elapsed.
- C. Implement an IAM policy to give the user read access to the S3 bucket.
- D. Create an S3 presigned URL Provide the S3 presigned URL to the user through the application.
- E. Create an Amazon CloudFront signed UR
- F. Provide the CloudFront signed URL to the user through the application.

**Answer: D**

#### Explanation:

For this scenario you would need to set up static website hosting because a custom domain name is listed as a requirement. "Amazon S3 website endpoints do not support HTTPS or access points. If you want to use HTTPS, you can use Amazon CloudFront to serve a static website hosted on Amazon S3." This is not secure. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/website-hosting-custom-domain-walkthrough.html> CloudFront signed URLs allow much more fine-grained control as well as HTTPS access with custom domain names:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>

#### NEW QUESTION 7

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

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

- A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication for the AL
- B. Define a SAML-based Amazon Cognito user pool and connect it to ADFS.
- C. Implement AWS SSO in the master account and link it to ADFS as an identity provide
- D. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.
- E. Define an Amazon Cognito identity pool, then install the connector on the Active Directory serve
- F. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their Active Directory user names and passwords.

G. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2. Ensure the security group on Amazon EC2 only allows access from the Lambda function.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>

#### NEW QUESTION 8

A company is running workloads in a single IAM account on Amazon EC2 instances and Amazon EMR clusters. A recent security audit revealed that multiple Amazon Elastic Block Store (Amazon EBS) volumes and snapshots are not encrypted. The company's security engineer is working on a solution that will allow users to deploy EC2 instances and EMR clusters while ensuring that all new EBS volumes and EBS snapshots are encrypted at rest. The solution must also minimize operational overhead. Which steps should the security engineer take to meet these requirements?

- A. Create an Amazon Event Bridge (Amazon CloudWatch Events) event with an EC2 instance as the source and create volume as the event trigger.
- B. When the event is triggered, invoke an IAM Lambda function to evaluate and notify the security engineer if the EBS volume that was created is not encrypted.
- C. Use a customer managed IAM policy that will verify that the encryption flag of the CreateVolume context is set to true.
- D. Apply this rule to all users.
- E. Create an IAM Config rule to evaluate the configuration of each EC2 instance on creation or modification. Have the IAM Config rule trigger an IAM Lambda function to alert the security team and terminate the instance if the EBS volume is not encrypted.
- F. 5
- G. Use the IAM Management Console or IAM CLI to enable encryption by default for EBS volumes in each IAM Region where the company operates.

**Answer:** D

**Explanation:**

To ensure that all new EBS volumes and EBS snapshots are encrypted at rest and minimize operational overhead, the security engineer should do the following:

- Use the AWS Management Console or AWS CLI to enable encryption by default for EBS volumes in each AWS Region where the company operates. This allows the security engineer to automatically encrypt any new EBS volumes and snapshots created from those volumes, without requiring any additional actions from users.

#### NEW QUESTION 9

A company uses SAML federation to grant users access to AWS accounts. A company workload that is in an isolated AWS account runs on immutable infrastructure with no human access to Amazon EC2. The company requires a specialized user known as a break glass user to have access to the workload AWS account and instances in the case of SAML errors. A recent audit discovered that the company did not create the break glass user for the AWS account that contains the workload.

The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team.

Which combination of solutions will meet these requirements? (Select TWO.)

- A. Create a local individual break glass IAM user for the security team.
- B. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on.
- C. Use Amazon EventBridge to monitor local user activities.
- D. Create a break glass EC2 key pair for the AWS account.
- E. Provide the key pair to the security team.
- F. Use AWS CloudTrail to monitor key pair activities.
- G. Send notifications to the security team by using Amazon Simple Notification Service (Amazon SNS).
- H. Create a break glass IAM role for the account.
- I. Allow security team members to perform the AssumeRoleWithSAML operation.
- J. Create an AWS CloudTrail trail that has Amazon CloudWatch Logs turned on.
- K. Use Amazon EventBridge to monitor security team activities.
- L. Create a local individual break glass IAM user on the operating system level of each workload instance. Configure unrestricted security groups on the instances to grant access to the break glass IAM users.
- M. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager.
- N. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic.

**Answer:** AE

**Explanation:**

The combination of solutions that will meet the requirements are:

- A. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities. This is a valid solution because it allows the security team to access the workload AWS account and instances using a local IAM user that does not depend on SAML federation. It also enables logging and monitoring of the break glass user activities using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon EventBridge.
  - E. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic. This is a valid solution because it allows the security team to access the workload instances without opening any inbound ports or managing SSH keys or bastion hosts. It also enables logging and notification of the break glass user activities using AWS CloudTrail, Session Manager, and Amazon SNS.
- The other options are incorrect because:
- B. Creating a break glass EC2 key pair for the AWS account and providing it to the security team is not a valid solution, because it requires opening inbound ports on the instances and managing SSH keys, which increases the security risk and complexity.
  - C. Creating a break glass IAM role for the account and allowing security team members to perform the AssumeRoleWithSAML operation is not a valid solution, because it still depends on SAML federation, which might not work in case of SAML errors.
  - D. Creating a local individual break glass IAM user on the operating system level of each workload instance and configuring unrestricted security groups on the instances to grant access to the break glass IAM users is not a valid solution, because it requires opening inbound ports on the instances and managing multiple local users, which increases the security risk and complexity.

References:

1: Creating an IAM User in Your AWS Account 2: Creating a Trail - AWS CloudTrail 3: Using Amazon EventBridge with AWS CloudTrail 4: Setting up Session Manager - AWS Systems Manager 5: Logging Session Manager sessions - AWS Systems Manager 6: Amazon Simple Notification Service 7: Connecting to your



Linux instance using SSH - Amazon Elastic Compute Cloud 8: AssumeRoleWithSAML - AWS Security Token Service 9: IAM Users - AWS Identity and Access Management

#### NEW QUESTION 10

A company is building an application on AWS that will store sensitive information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated. What should the security engineer recommend?

- A. Enable Amazon RDS encryption to encrypt the database and snapshot
- B. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
- C. Include the database credential in the EC2 user data field
- D. Use an AWS Lambda function to rotate database credential
- E. Set up TLS for the connection to the database.
- F. Install a database on an Amazon EC2 instance
- G. Enable third-party disk encryption to encrypt Amazon Elastic Block Store (Amazon EBS) volume
- H. Store the database credentials in AWS CloudHSM with automatic rotation
- I. Set up TLS for the connection to the database.
- J. Enable Amazon RDS encryption to encrypt the database and snapshot
- K. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
- L. Store the database credentials in AWS Secrets Manager with automatic rotation
- M. Set up TLS for the connection to the RDS hosted database.
- N. Set up an AWS CloudHSM cluster with AWS Key Management Service (AWS KMS) to store KMS key
- O. Set up Amazon RDS encryption using AWS KMS to encrypt the database
- P. Store the database credentials in AWS Systems Manager Parameter Store with automatic rotation
- Q. Set up TLS for the connection to the RDS hosted database.

**Answer: C**

#### NEW QUESTION 10

A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company's security policies for accessing other AWS resources from Amazon EC2.

A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLE-BUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.

The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).

Which combination of steps should the security engineer take to gather this information? (Choose two.)

- A. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- B. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- C. Use Amazon OpenSearch Service (Amazon Elasticsearch Service) to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for API calls that used the access key to access an object that contained PII.
- D. Use Amazon Athena to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for any API calls that used the access key to access an object that contained PII.
- E. Use AWS Identity and Access Management Access Analyzer to identify any API calls that used the access key to access objects that contained PII in DOC-EXAMPLE-BUCKET1.

**Answer: AD**

#### NEW QUESTION 13

A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.

The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.

Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

- A. Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.
- B. Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.
- C. Create an EC2 key pair
- D. Associate the key pair with the EC2 instance.
- E. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
- F. Attach a security group to the VPC interface endpoint
- G. Allow inbound traffic on port 443 to the VPC's CIDR range.
- H. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

**Answer: BCF**

#### NEW QUESTION 16

A security engineer needs to implement a write-once-read-many (WORM) model for data that a company will store in Amazon S3 buckets. The company uses the S3 Standard storage class for all of its S3 buckets. The security engineer must ensure that objects cannot be overwritten or deleted by any user, including the AWS account root user.

Which solution will meet these requirements?

- A. Create new S3 buckets with S3 Object Lock enabled in compliance mode
- B. Place objects in the S3 buckets.
- C. Use S3 Glacier Vault Lock to attach a Vault Lock policy to new S3 bucket

- D. Wait 24 hours to complete the Vault Lock proces
- E. Place objects in the S3 buckets.
- F. Create new S3 buckets with S3 Object Lock enabled in governance mod
- G. Place objects in the S3 buckets.
- H. Create new S3 buckets with S3 Object Lock enabled in governance mod
- I. Add a legal hold to the S3 bucket
- J. Place objects in the S3 buckets.

**Answer:** A

#### NEW QUESTION 18

Your company is planning on using bastion hosts for administering the servers in IAM. Which of the following is the best description of a bastion host from a security perspective?

Please select:

- A. A Bastion host should be on a private subnet and never a public subnet due to security concerns
- B. A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network
- C. Bastion hosts allow users to log in using RDP or SSH and use that session to S5H into internal network to access private subnet resources.
- D. A Bastion host should maintain extremely tight security and monitoring as it is available to the public

**Answer:** C

#### Explanation:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

In IAM, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring For more information on bastion hosts, just browse to the below URL:

<https://docsIAM.amazon.com/quickstart/latest/linux-bastion/architecture.html>

The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 19

A security team is working on a solution that will use Amazon EventBridge (Amazon CloudWatch Events) to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.

Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event. However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.

The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested.

Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.

Which solution will meet these requirements?

- A. Modify the EventBridge event pattern by selecting Amazon S3. Select All Events as the event type.
- B. Modify the EventBridge event pattern by selecting Amazon S3. Select Bucket Level Operations as the event type.
- C. Enable CloudTrail Insights to identify unusual API activity.
- D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets.

**Answer:** D

#### Explanation:

The correct answer is D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets. According to the AWS documentation<sup>1</sup>, CloudTrail data events are the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities. For example, Amazon S3 object-level API activity (such as GetObject, DeleteObject, and PutObject) is a data event.

By default, trails do not log data events. To record CloudTrail data events, you must explicitly add the supported resources or resource types for which you want to collect activity. For more information, see Logging data events in the Amazon S3 User Guide<sup>2</sup>.

In this case, the security team wants EventBridge to watch for the s3:PutObjectAcl API invocation logs from CloudTrail. This API uses the acl subresource to set the access control list (ACL) permissions for a new or existing object in an S3 bucket<sup>3</sup>. This is a data event that affects the S3 object resource type. Therefore, the security team must enable CloudTrail to monitor data events for read and write operations to S3 buckets in order to invoke an EventBridge event for this API call.

The other options are incorrect because:

- A. Modifying the EventBridge event pattern by selecting Amazon S3 and All Events as the event type will not capture the s3:PutObjectAcl API call, because this is a data event and not a management event. Management events provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations<sup>4</sup>.
- B. Modifying the EventBridge event pattern by selecting Amazon S3 and Bucket Level Operations as the event type will not capture the s3:PutObjectAcl API call, because this is a data event that affects the S3 object resource type and not the S3 bucket resource type. Bucket level operations are management events that affect the configuration or metadata of an S3 bucket<sup>5</sup>.
- C. Enabling CloudTrail Insights to identify unusual API activity will not help the security team monitor new S3 objects or changes to any S3 bucket policy or setting that result in public access. CloudTrail Insights helps AWS users identify and respond to unusual activity associated with API calls and API error rates by continuously analyzing CloudTrail management events<sup>6</sup>. It does not analyze data events or generate EventBridge events.

References:

1: CloudTrail log event reference - AWS CloudTrail 2: Logging data events - AWS CloudTrail 3: PutObjectAcl - Amazon Simple Storage Service 4: [Logging management events - AWS CloudTrail] 5: [Amazon S3 Event Types - Amazon Simple Storage Service] 6: Logging Insights events for trails - AWS CloudTrail

#### NEW QUESTION 24

A Network Load Balancer (NLB) target instance is not entering the InService state. A security engineer determines that health checks are failing.

Which factors could cause the health check failures? (Select THREE.)

- A. The target instance's security group does not allow traffic from the NLB.
- B. The target instance's security group is not attached to the NLB.
- C. The NLB's security group is not attached to the target instance.
- D. The target instance's subnet network ACL does not allow traffic from the NLB.
- E. The target instance's security group is not using IP addresses to allow traffic from the NLB.
- F. The target network ACL is not attached to the NLB.

**Answer:** ACD

#### NEW QUESTION 26

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. A computer code with black text Description automatically generated

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

C. A computer code with black text Description automatically generated

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

D. A computer code with text Description automatically generated

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

**Answer:** C

**Explanation:**

[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_examples\\_aws\\_deny-requested-region.h](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.html)

**NEW QUESTION 30**

A company wants to remove all SSH keys permanently from a specific subset of its Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile. However, three individuals who have IAM user accounts will need to access these instances by using an SSH session to perform critical duties. How can a security engineer provide the access to meet these requirements?

- A. Assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager. Provide the IAM user accounts with permission to use Systems Manager. Remove the SSH keys from the EC2 instances. Use Systems Manager Inventory to select the EC2 instance and connect.
- B. Assign an IAM policy to the IAM user accounts to provide permission to use AWS Systems Manager. Run Command. Remove the SSH keys from the EC2 instances. Use Run Command to open an SSH connection to the EC2 instance.
- C. Assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager. Provide the IAM user accounts with permission to use Systems Manager. Remove the SSH keys from the EC2 instances. Use Systems Manager Session Manager to select the EC2 instance and connect.
- D. Assign an IAM policy to the IAM user accounts to provide permission to use the EC2 service in the AWS Management Console. Remove the SSH keys from the EC2 instances. Connect to the EC2 instance as the ec2-user through the AWS Management Console's EC2 SSH client method.

**Answer:** C

**Explanation:**

To provide access to the three individuals who have IAM user accounts to access the Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile, the most appropriate solution would be to assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager, provide the IAM user accounts with permission to use Systems Manager, remove the SSH keys from the EC2 instances, and use Systems Manager Session Manager to select the EC2 instance and connect.

References: : AWS Systems Manager Session Manager - AWS Systems Manager : AWS Systems Manager AWS Management Console : AWS Identity and Access Management - AWS Management Console : Amazon Elastic Compute Cloud - Amazon Web Services : Amazon Linux 2 - Amazon Web Services : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console

**NEW QUESTION 34**

A company uses AWS Organizations and has production workloads across multiple AWS accounts. A security engineer needs to design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads.

The solution must automate remediation of incidents across the production accounts. The solution also must publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic when a critical security finding is detected. In addition, the solution must send all security incident logs to a dedicated account.

Which solution will meet these requirements?

- A. Activate Amazon GuardDuty in each production account.
- B. In a dedicated logging account.
- C. Aggregate all GuardDuty logs from each production account.
- D. Remediate incidents by configuring GuardDuty to directly invoke an AWS Lambda function.
- E. Configure the Lambda function to also publish notifications to the SNS topic.
- F. Activate AWS Security Hub in each production account.
- G. In a dedicated logging account.
- H. Aggregate all Security Hub findings from each production account.
- I. Remediate incidents by using AWS Config and AWS Systems Manager.
- J. Configure Systems Manager to also publish notifications to the SNS topic.
- K. Activate Amazon GuardDuty in each production account.
- L. In a dedicated logging account.
- M. Aggregate all GuardDuty logs from each production account. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the GuardDuty finding.
- N. Configure the Lambda function to also publish notifications to the SNS topic.
- O. Activate AWS Security Hub in each production account.
- P. In a dedicated logging account.
- Q. Aggregate all Security Hub findings from each production account.



- R. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the Security Hub finding
- S. Configure the Lambda function to also publish notifications to the SNS topic.

**Answer:** D

**Explanation:**

The correct answer is D.

To design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads, the security engineer needs to use a service that can aggregate and analyze security findings from multiple sources. AWS Security Hub is a service that provides a comprehensive view of your security posture across your AWS accounts and enables you to check your environment against security standards and best practices. Security Hub also integrates with other AWS services, such as Amazon GuardDuty, AWS Config, and AWS Systems Manager, to collect and correlate security findings.

To automate remediation of incidents across the production accounts, the security engineer needs to use a service that can trigger actions based on events.

Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from a variety of sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke a custom AWS Lambda function from the Security Hub findings.

Lambda is a serverless compute service that lets you run code without provisioning or managing servers.

To publish a notification to an Amazon SNS topic when a critical security finding is detected, the security engineer needs to use a service that can send messages to subscribers. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can configure the Lambda function to also publish notifications to the SNS topic.

To send all security incident logs to a dedicated account, the security engineer needs to use a service that can aggregate and store log data from multiple sources. AWS Security Hub allows you to aggregate security findings from multiple accounts into a single account using the delegated administrator feature. This feature enables you to designate an AWS account as the administrator for Security Hub in an organization. The administrator account can then view and manage Security Hub findings from all member accounts.

Therefore, option D is correct because it meets all the requirements of the solution. Option A is incorrect because GuardDuty does not provide a comprehensive view of your security posture across your AWS accounts. GuardDuty is primarily a threat detection service that monitors for malicious or unauthorized behavior.

Option B is incorrect because Config and Systems Manager are not designed to automate remediation of incidents based on Security Hub findings. Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources, while Systems Manager is a service that allows you to manage your infrastructure on AWS at scale. Option C is incorrect because GuardDuty does not provide a comprehensive view of your security posture across your AWS accounts.

References:

- AWS Security Hub
- Amazon EventBridge
- AWS Lambda
- Amazon SNS
- Aggregating Security Hub findings across accounts

**NEW QUESTION 38**

A security engineer is defining the controls required to protect the IAM account root user credentials in an IAM Organizations hierarchy. The controls should also limit the impact in case these credentials have been compromised.

Which combination of controls should the security engineer propose? (Select THREE.)

A)

Apply the following SCP:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRRESTRICTROOTUSER",
      "Effect": "Deny",
      "Action": "*",
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

B)

Apply the following SCP:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRRESTRICTROOTUSER",
      "Effect": "Deny",
      "Principal": "arn:aws:iam::*:root",
      "Action": "*",
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- C) Enable multi-factor authentication (MFA) for the root user.
- D) Set a strong randomized password and store it in a secure location.
- E) Create an access key ID and secret access key, and store them in a secure location.
- F) Apply the following permissions boundary to the root user:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRRESTRICTROOTUSER",
      "Effect": "Deny",
      "Action": "*",
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E
- F. Option F

**Answer:** ACE

#### NEW QUESTION 40

A security engineer receives a notice from the AWS Abuse team about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS)-based storage. The instance is making connections to known malicious addresses.

The instance is in a development account within a VPC that is in the us-east-1 Region. The VPC contains an internet gateway and has a subnet in us-east-1a and us-east-1b. Each subnet is associated with a route table that uses the internet gateway as a default route. Each subnet also uses the default network ACL. The suspicious EC2 instance runs within the us-east-1b subnet. During an initial investigation, a security engineer discovers that the suspicious instance is the only instance that runs in the subnet.

Which response will immediately mitigate the attack and help investigate the root cause?

- A. Log in to the suspicious instance and use the netstat command to identify remote connections. Use the IP addresses from these remote connections to create deny rules in the security group of the instance. Install diagnostic tools on the instance for investigation. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule during the investigation of the instance.
- B. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule. Replace the security group with a new security group that allows connections only from a diagnostics security group. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rule. Launch a new EC2 instance that has diagnostic tools. Assign the new security group to the new EC2 instance. Use the new EC2 instance to investigate the suspicious instance.
- C. Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon termination. Terminate the instance. Launch a new EC2 instance in us-east-1a that has diagnostic tools. Mount the EBS volumes from the terminated instance for investigation.
- D. Create an AWS WAF web ACL that denies traffic to and from the suspicious instance. Attach the AWS WAF web ACL to the instance to mitigate the attack. Log in to the instance and install diagnostic tools to investigate the instance.

**Answer:** B

#### Explanation:

This option suggests updating the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule, replacing the security group.

with a new one that only allows connections from a diagnostics security group, and launching a new EC2 instance with diagnostic tools to investigate the suspicious instance. This option will immediately mitigate the attack and provide the necessary tools for investigation.

#### NEW QUESTION 44

A company purchased a subscription to a third-party cloud security scanning solution that integrates with AWS Security Hub. A security engineer needs to implement a solution that will remediate the findings from the third-party scanning solution automatically. Which solution will meet this requirement?

- A. Set up an Amazon EventBridge rule that reacts to new Security Hub find-ing
- B. Configure an AWS Lambda function as the target for the rule to reme-diate the findings.
- C. Set up a custom action in Security Hu
- D. Configure the custom action to call AWS Systems Manager Automation runbooks to remediate the findings.
- E. Set up a custom action in Security Hu
- F. Configure an AWS Lambda function as the target for the custom action to remediate the findings.
- G. Set up AWS Config rules to use AWS Systems Manager Automation runbooks to remediate the findings.

**Answer:** A

#### NEW QUESTION 45

A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised. How can a security engineer meet this requirement?

- A. Create an HTTPS listener that uses a certificate that is managed by IAM Certificate Manager (ACM).
- B. Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect toward secrecy (PFS).
- C. Create an HTTPS listener that uses the Server Order Preference security feature.
- D. Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).

**Answer:** A

#### NEW QUESTION 46

A company is using IAM Secrets Manager to store secrets for its production Amazon RDS database. The Security Officer has asked that secrets be rotated every 3 months. Which solution would allow the company to securely rotate the secrets? (Select TWO.)

- A. Place the RDS instance in a public subnet and an IAM Lambda function outside the VP
- B. Schedule the Lambda function to run every 3 months to rotate the secrets.
- C. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subne
- D. Configure the private subnet to use a NAT gatewa
- E. Schedule the Lambda function to run every 3 months to rotate the secrets.
- F. Place the RDS instance in a private subnet and an IAM Lambda function outside the VP
- G. Configure the private subnet to use an internet gatewa
- H. Schedule the Lambda function to run every 3 months lo rotate the secrets.
- I. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subne
- J. Schedule the Lambda function to run quarterly to rotate the secrets.
- K. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subne
- L. Configure a Secrets Manager interface endpoint
- M. Schedule the Lambda function to run every 3 months to rotate the secrets.

**Answer:** BE

#### Explanation:

these are the solutions that can securely rotate the secrets for the production RDS database using Secrets Manager. Secrets Manager is a service that helps you manage secrets such as database credentials, API keys, and passwords. You can use Secrets Manager to rotate secrets automatically by using a Lambda function that runs on a schedule. The Lambda function needs to have access to both the RDS instance and the Secrets Manager service. Option B places the RDS instance in a private subnet and the Lambda function in the same VPC in another private subnet. The private subnet with the Lambda function needs to use a NAT gateway to access Secrets Manager over the internet. Option E places the RDS instance and the Lambda function in the same private subnet and configures a Secrets Manager interface endpoint, which is a private connection between the VPC and Secrets Manager. The other options are either insecure or incorrect for rotating secrets using Secrets Manager.

#### NEW QUESTION 51

A company uses AWS Organizations. The company wants to implement short-term cre-dentials for third-party AWS accounts to use to access accounts within the com-pany's organization. Access is for the AWS Management Console and third-party software-as-a-service (SaaS) applications. Trust must be enhanced to prevent two external accounts from using the same credentials. The solution must require the least possible operational effort. Which solution will meet these requirements?

- A. Use a bearer token authentication with OAuth or SAML to manage and share a central Amazon Cognito user pool across multiple Amazon API Gateway APIs.
- B. Implement AWS IAM Identity Center (AWS Single Sign-On), and use an identi-ty source of choice. Grant access to users and groups from other accounts by using permission sets that are assigned by account.
- C. Create a unique IAM role for each external accoun
- D. Create a trust polic
- E. Use AWS Secrets Manager to create a random external key.
- F. Create a unique IAM role for each external accoun
- G. Create a trust policy that includes a condition that uses the sts:ExternalId condition key.

**Answer:** D

#### Explanation:

The correct answer is D.

To implement short-term credentials for third-party AWS accounts, you can use IAM roles and trust policies. A trust policy is a JSON policy document that defines

who can assume the role. You can specify the AWS account ID of the third-party account as a principal in the trust policy, and use the sts:ExternalId condition key to enhance the security of the role. The sts:ExternalId condition key is a unique identifier that is agreed upon by both parties and included in the AssumeRole request. This way, you can prevent the “confused deputy” problem, where an unauthorized party can use the same role as a legitimate party. Option A is incorrect because bearer token authentication with OAuth or SAML is not suitable for granting access to AWS accounts and resources. Amazon Cognito and API Gateway are used for building web and mobile applications that require user authentication and authorization. Option B is incorrect because AWS IAM Identity Center (AWS Single Sign-On) is a service that simplifies the management of access to multiple AWS accounts and cloud applications for your workforce users. It does not support granting access to third-party AWS accounts. Option C is incorrect because using AWS Secrets Manager to create a random external key is not necessary and adds operational complexity. You can use the sts:ExternalId condition key instead to provide a unique identifier for each external account.

#### NEW QUESTION 54

A security engineer is designing an IAM policy for a script that will use the AWS CLI. The script currently assumes an IAM role that is attached to three AWS managed IAM policies: AmazonEC2FullAccess, AmazonDynamoDBFullAccess, and AmazonVPCFullAccess. The security engineer needs to construct a least privilege IAM policy that will replace the AWS managed IAM policies that are attached to this role. Which solution will meet these requirements in the MOST operationally efficient way?

- A. In AWS CloudTrail, create a trail for management event
- B. Run the script with the existing AWS managed IAM policies
- C. Use IAM Access Analyzer to generate a new IAM policy that is based on access activity in the trail
- D. Replace the existing AWS managed IAM policies with the generated IAM policy for the role.
- E. Remove the existing AWS managed IAM policies from the role
- F. Attach the IAM Access Analyzer Role Policy Generator to the role
- G. Run the script
- H. Return to IAM Access Analyzer and generate a least privilege IAM policy
- I. Attach the new IAM policy to the role.
- J. Create an account analyzer in IAM Access Analyzer
- K. Create an archive rule that has a filter that checks whether the PrincipalArn value matches the ARN of the role
- L. Run the script
- M. Remove the existing AWS managed IAM policies from the role.
- N. In AWS CloudTrail, create a trail for management event
- O. Remove the existing AWS managed IAM policies from the role
- P. Run the script
- Q. Find the authorization failure in the trail event that is associated with the script
- R. Create a new IAM policy that includes the action and resource that caused the authorization failure
- S. Repeat the process until the script succeeds
- T. Attach the new IAM policy to the role.

**Answer:** A

#### NEW QUESTION 57

A company has an AWS account that includes an Amazon S3 bucket. The S3 bucket uses server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all the objects at rest by using a customer managed key. The S3 bucket does not have a bucket policy. An IAM role in the same account has an IAM policy that allows s3:List\* and s3:Get\* permissions for the S3 bucket. When the IAM role attempts to access an object in the S3 bucket the role receives an access denied message. Why does the IAM role not have access to the objects that are in the S3 bucket?

- A. The IAM role does not have permission to use the KMS CreateKey operation.
- B. The S3 bucket lacks a policy that allows access to the customer managed key that encrypts the objects.
- C. The IAM role does not have permission to use the customer managed key that encrypts the objects that are in the S3 bucket.
- D. The ACL of the S3 objects does not allow read access for the objects when the objects are encrypted at rest.

**Answer:** C

#### Explanation:

When using server-side encryption with AWS KMS keys (SSE-KMS), the requester must have both Amazon S3 permissions and AWS KMS permissions to access the objects. The Amazon S3 permissions are for the bucket and object operations, such as s3:ListBucket and s3:GetObject. The AWS KMS permissions are for the key operations, such as kms:GenerateDataKey and kms:Decrypt. In this case, the IAM role has the necessary Amazon S3 permissions, but not the AWS KMS permissions to use the customer managed key that encrypts the objects. Therefore, the IAM role receives an access denied message when trying to access the objects. Verified References:

- > <https://docs.aws.amazon.com/AmazonS3/latest/userguide/troubleshoot-403-errors.html>
- > <https://repost.aws/knowledge-center/s3-access-denied-error-kms>
- > <https://repost.aws/knowledge-center/cross-account-access-denied-error-s3>

#### NEW QUESTION 60

A company maintains an open-source application that is hosted on a public GitHub repository. While creating a new commit to the repository, an engineer uploaded their IAM access key and secret access key. The engineer reported the mistake to a manager, and the manager immediately disabled the access key. The company needs to assess the impact of the exposed access key. A security engineer must recommend a solution that requires the least possible managerial overhead. Which solution meets these requirements?

- A. Analyze an IAM Identity and Access Management (IAM) use report from IAM Trusted Advisor to see when the access key was last used.
- B. Analyze Amazon CloudWatch Logs for activity by searching for the access key.
- C. Analyze VPC flow logs for activity by searching for the access key
- D. Analyze a credential report in IAM Identity and Access Management (IAM) to see when the access key was last used.

**Answer:** A

#### Explanation:

To assess the impact of the exposed access key, the security engineer should recommend the following solution:



➤ Analyze an IAM use report from AWS Trusted Advisor to see when the access key was last used. This allows the security engineer to use a tool that provides information about IAM entities and credentials in their account, and check if there was any unauthorized activity with the exposed access key.

#### NEW QUESTION 63

An IAM user receives an Access Denied message when the user attempts to access objects in an Amazon S3 bucket. The user and the S3 bucket are in the same AWS account. The S3 bucket is configured to use server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all of its objects at rest by using a customer managed key from the same AWS account. The S3 bucket has no bucket policy defined. The IAM user has been granted permissions through an IAM policy that allows the kms:Decrypt permission to the customer managed key. The IAM policy also allows the s3:List\* and s3:Get\* permissions for the S3 bucket and its objects.

Which of the following is a possible reason that the IAM user cannot access the objects in the S3 bucket?

- A. The IAM policy needs to allow the kms:DescribeKey permission.
- B. The S3 bucket has been changed to use the AWS managed key to encrypt objects at rest.
- C. An S3 bucket policy needs to be added to allow the IAM user to access the objects.
- D. The KMS key policy has been edited to remove the ability for the AWS account to have full access to the key.

**Answer: D**

#### Explanation:

The possible reason that the IAM user cannot access the objects in the S3 bucket is D. The KMS key policy has been edited to remove the ability for the AWS account to have full access to the key.

This answer is correct because the KMS key policy is the primary way to control access to the KMS key, and it must explicitly allow the AWS account to have full access to the key. If the KMS key policy has been edited to remove this permission, then the IAM policy that grants kms:Decrypt permission to the IAM user has no effect, and the IAM user cannot decrypt the objects in the S3 bucket<sup>12</sup>.

The other options are incorrect because:

- A. The IAM policy does not need to allow the kms:DescribeKey permission, because this permission is not required for decrypting objects in S3 using SSE-KMS. The kms:DescribeKey permission allows getting information about a KMS key, such as its creation date, description, and key state<sup>3</sup>.
- B. The S3 bucket has not been changed to use the AWS managed key to encrypt objects at rest, because this would not cause an Access Denied message for the IAM user. The AWS managed key is a default KMS key that is created and managed by AWS for each AWS account and Region. The IAM user does not need any permissions on this key to use it for SSE-KMS<sup>4</sup>.
- C. An S3 bucket policy does not need to be added to allow the IAM user to access the objects, because the IAM user already has s3:List\* and s3:Get\* permissions for the S3 bucket and its objects through an IAM policy. An S3 bucket policy is an optional way to grant cross-account access or public access to an S3 bucket<sup>5</sup>.

References:

1: Key policies in AWS KMS 2: Using server-side encryption with AWS KMS keys (SSE-KMS) 3: AWS KMS API Permissions Reference 4: Using server-side encryption with Amazon S3 managed keys (SSE-S3) 5: Bucket policy examples

#### NEW QUESTION 64

Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.

Please select:

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

```
"Version": "2012-10-17",
  "Id": "PutObj",
  "Statement": [
    {
      "Sid": "DenyUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::demo/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "aws:kms"
        }
      }
    }
  ]
}
```

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

```
"Version": "2012-10-17",
"Id": "PutObj",
"Statement": [
  {
    "Sid": "DenyUploads",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::demo/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-server-side-encryption": "aws:kms"
      }
    }
  }
]
```

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

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

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

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

**Answer:** A

**Explanation:**

The condition of "s3:x-amz-server-side-encryption":"IAM:kms" ensures that objects uploaded need to be encrypted.

Options B,C and D are invalid because you have to ensure the condition of ns3:x-amz-server-side-encryption":"IAM:kms" is present

For more information on IAM KMS best practices, just browse to the below URL: <https://dl.IAMstatic.com/whitepapers/IAM-kms-best-praactices.pdf>

Submit your Feedback/Queries to our Expert

**NEW QUESTION 67**

A company is using AWS WAF to protect a customized public API service that is based on Amazon EC2 instances. The API uses an Application Load Balancer. The AWS WAF web ACL is configured with an AWS Managed Rules rule group. After a software upgrade to the API and the client application, some types of requests are no longer working and are causing application stability issues. A security engineer discovers that AWS WAF logging is not turned on for the web ACL. The security engineer needs to immediately return the application to service, resolve the issue, and ensure that logging is not turned off in the future. The security engineer turns on logging for the web ACL and specifies Amazon Cloud-Watch Logs as the destination. Which additional set of steps should the security engineer take to meet the re-quirements?

- A. Edit the rules in the web ACL to include rules with Count action
- B. Review the logs to determine which rule is blocking the reques
- C. Modify the IAM policy of all AWS WAF administrators so that they cannot remove the log-ging configuration for any AWS WAF web ACLs.
- D. Edit the rules in the web ACL to include rules with Count action
- E. Review the logs to determine which rule is blocking the reques
- F. Modify the AWS WAF resource policy so that AWS WAF administrators cannot remove the log-ging configuration for any AWS WAF web ACLs.
- G. Edit the rules in the web ACL to include rules with Count and Challenge action
- H. Review the logs to determine which rule is blocking the reques
- I. Modify the AWS WAF resource policy so that AWS WAF administrators cannot remove the logging configuration for any AWS WAF web ACLs.

- J. Edit the rules in the web ACL to include rules with Count and Challenge action
- K. Review the logs to determine which rule is blocking the request
- L. Modify the IAM policy of all AWS WAF administrators so that they cannot remove the logging configuration for any AWS WAF web ACLs.

**Answer:** A

**Explanation:**

This answer is correct because it meets the requirements of returning the application to service, resolving the issue, and ensuring that logging is not turned off in the future. By editing the rules in the web ACL to include rules with Count actions, the security engineer can test the effect of each rule without blocking or allowing requests. By reviewing the logs, the security engineer can identify which rule is causing the problem and modify or delete it accordingly. By modifying the IAM policy of all AWS WAF administrators, the security engineer can restrict their permissions to prevent them from removing the logging configuration for any AWS WAF web ACLs.

**NEW QUESTION 69**

A company's security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.

Which solution will meet these requirements with the LEAST amount of effort?

- A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hours
- B. Select the access-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 days
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with an event pattern that matches the compliance type of NON\_COMPLIANT from AWS Config for the managed rule
- D. Configure EventBridge (CloudWatch Events) to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- E. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation. Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucket
- F. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucket
- G. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- H. Create a script to download the IAM credentials report on a periodic basis
- I. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge (Amazon CloudWatch Events). Configure the Lambda script to load the report into memory and to filter the report for records in which the key was last rotated at least 90 days ago
- J. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- K. Create an AWS Lambda function that queries the IAM API to list all the users
- L. Iterate through the users by using the ListAccessKeys operation
- M. Verify that the value in the CreateDate field is not at least 90 days old
- N. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days old
- O. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule the Lambda function to run each day.

**Answer:** A

**NEW QUESTION 74**

A security engineer needs to create an IAM Key Management Service (IAM KMS) key that will be used to encrypt all data stored in a company's Amazon S3 Buckets in the us-west-1 Region. The key will use

server-side encryption. Usage of the key must be limited to requests coming from Amazon S3 within the company's account.

Which statement in the KMS key policy will meet these requirements?

A)

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "s3.us-west-1.amazonaws.com",
      "kms:CallerAccount": "<CustomerAccountID>"
    }
  }
}
```

B)

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "s3.us-west-1.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:CallerAccount": "<CustomerAccountID>"
    }
  }
}
```

C)

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::"
      ]
    }
  }
}
```

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

**Answer:** A**NEW QUESTION 79**

A company uses Amazon EC2 Linux instances in the AWS Cloud. A member of the company's security team recently received a report about common vulnerability identifiers on the instances.

A security engineer needs to verify patching and perform remediation if the instances do not have the correct patches installed. The security engineer must determine which EC2 instances are at risk and must implement a solution to automatically update those instances with the applicable patches.

What should the security engineer do to meet these requirements?

- A. Use AWS Systems Manager Patch Manager to view vulnerability identifiers for missing patches on the instance
- B. Use Patch Manager also to automate the patching process.
- C. Use AWS Shield Advanced to view vulnerability identifiers for missing patches on the instance
- D. Use AWS Systems Manager Patch Manager to automate the patching process.
- E. Use Amazon GuardDuty to view vulnerability identifiers for missing patches on the instance
- F. Use Amazon Inspector to automate the patching process.
- G. Use Amazon Inspector to view vulnerability identifiers for missing patches on the instance
- H. Use Amazon Inspector also to automate the patching process.

**Answer:** A**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2020/10/now-use-aws-systems-manager-to-view-vulnerability-id>

**NEW QUESTION 81**

A company hosts multiple externally facing applications, each isolated in its own IAM account. The company's Security team has enabled IAM WAF, IAM Config, and Amazon GuardDuty on all accounts. The company's Operations team has also joined all of the accounts to IAM Organizations and established centralized logging for CloudTrail, IAM Config, and GuardDuty. The company wants the Security team to take a reactive remediation in one account, and automate implementing this remediation as proactive prevention in all the other accounts.

How should the Security team accomplish this?

- A. Update the IAM WAF rules in the affected account and use IAM Firewall Manager to push updated IAM WAF rules across all other accounts.



- B. Use GuardDuty centralized logging and Amazon SNS to set up alerts to notify all application teams of security incidents.
- C. Use GuardDuty alerts to write an IAM Lambda function that updates all accounts by adding additional NACLs on the Amazon EC2 instances to block known malicious IP addresses.
- D. Use IAM Shield Advanced to identify threats in each individual account and then apply the account-based protections to all other accounts through Organizations.

Answer: C

#### NEW QUESTION 86

A company has a guideline that mandates the encryption of all Amazon S3 bucket data in transit. A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted. Which S3 bucket policy will meet this requirement?

- A. 

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowSSLRequestOnly",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    ],
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "true"
      }
    },
    "Principal": "*"
  }]
}
```
- B. 

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowSSLRequestOnly",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    ],
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    },
    "Principal": "*"
  }]
}
```
- C. 

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowSSLRequestOnly",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    ],
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    },
    "Principal": "*"
  }]
}
```
- D. A screenshot of a computer code Description automatically generated

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowSSLRequestOnly",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    ],
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": true
      }
    },
    "Principal": "*"
  }]
}
```

**Answer:** B

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-y>

**NEW QUESTION 88**

A company's security engineer is designing an isolation procedure for Amazon EC2 instances as part of an incident response plan. The security engineer needs to isolate a target instance to block any traffic to and from the target instance, except for traffic from the company's forensics team. Each of the company's EC2 instances has its own dedicated security group. The EC2 instances are deployed in subnets of a VPC. A subnet can contain multiple instances.

The security engineer is testing the procedure for EC2 isolation and opens an SSH session to the target instance. The procedure starts to simulate access to the target instance by an attacker. The security engineer removes the existing security group rules and adds security group rules to give the forensics team access to the target instance on port 22.

After these changes, the security engineer notices that the SSH connection is still active and usable. When the security engineer runs a ping command to the public IP address of the target instance, the ping command is blocked.

What should the security engineer do to isolate the target instance?

- A. Add an inbound rule to the security group to allow traffic from 0.0.0.0/0 for all port
- B. Add an outbound rule to the security group to allow traffic to 0.0.0.0/0 for all port
- C. Then immediately delete these rules.
- D. Remove the port 22 security group rule
- E. Attach an instance role policy that allows AWS Systems Manager Session Manager connections so that the forensics team can access the target instance.
- F. Create a network ACL that is associated with the target instance's subnet
- G. Add a rule at the top of the inbound rule set to deny all traffic from 0.0.0.0/0. Add a rule at the top of the outbound rule set to deny all traffic to 0.0.0.0/0.
- H. Create an AWS Systems Manager document that adds a host-level firewall rule to block all inbound traffic and outbound traffic
- I. Run the document on the target instance.

**Answer:** C

**NEW QUESTION 91**

A company became aware that one of its access keys was exposed on a code sharing website 11 days ago. A Security Engineer must review all use of the exposed access keys to determine the extent of the exposure. The company enabled IAM CloudTrail in all regions when it opened the account. Which of the following will allow the Security Engineer to complete the task?

- A. Filter the event history on the exposed access key in the CloudTrail console. Examine the data from the past 11 days.
- B. Use the IAM CLI to generate an IAM credential report. Extract all the data from the past 11 days.
- C. Use Amazon Athena to query the CloudTrail logs from Amazon S3. Retrieve the rows for the exposed access key for the past 11 days.
- D. Use the Access Advisor tab in the IAM console to view all of the access key activity for the past 11 days.

**Answer:** C

**Explanation:**

Amazon Athena is a service that enables you to analyze data in Amazon S3 using standard SQL. You can use Athena to query the CloudTrail logs that are stored in S3 and filter them by the exposed access key and the date range. The other options are not effective ways to review the use of the exposed access key.

**NEW QUESTION 95**

A company uses several AWS CloudFormation stacks to handle the deployment of a suite of applications. The leader of the company's application development team notices that the stack deployments fail with permission errors when some team members try to deploy the stacks. However, other team members can deploy the stacks successfully.

The team members access the account by assuming a role that has a specific set of permissions that are necessary for the job responsibilities of the team members. All team members have permissions to perform operations on the stacks.

Which combination of steps will ensure consistent deployment of the stacks MOST securely? (Select THREE.)

- A. Create a service role that has a composite principal that contains each service that needs the necessary permission
- B. Configure the role to allow the sts:AssumeRole action.
- C. Create a service role that has cloudformation.amazonaws.com as the service principal
- D. Configure the role to allow the sts:AssumeRole action.
- E. For each required set of permissions, add a separate policy to the role to allow those permissions
- F. Add the ARN of each CloudFormation stack in the resource field of each policy.
- G. For each required set of permissions, add a separate policy to the role to allow those permissions
- H. Add the ARN of each service that needs the permissions in the resource field of the corresponding policy.
- I. Update each stack to use the service role.

- J. Add a policy to each member role to allow the iam:PassRole action.
- K. Set the policy's resource field to the ARN of the service role.

**Answer:** BDF

#### NEW QUESTION 97

A security engineer logs in to the AWS Lambda console with administrator permissions. The security engineer is trying to view logs in Amazon CloudWatch for a Lambda function that is named myFunction.

When the security engineer chooses the option in the Lambda console to view logs in CloudWatch, an "error loading Log Streams" message appears.

The IAM policy for the Lambda function's execution role contains the following:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "logs:CreateLogGroup",
      "Resource": "arn:aws:logs:us-east-1:111111111111:*"
    },
    {
      "Effect": "Allow",
      "Action": ["logs:PutLogEvents"],
      "Resource": ["arn:aws:logs:us-east-1:111111111111:log-
group:/aws/Lambda/myFunction:*"]
    }
  ]
}
```

How should the security engineer correct the error?

- A. Move the logs:CreateLogGroup action to the second Allow statement.
- B. Add the logs:PutDestination action to the second Allow statement.
- C. Add the logs:GetLogEvents action to the second Allow statement.
- D. Add the logs:CreateLogStream action to the second Allow statement.

**Answer:** D

#### Explanation:

CloudWatchLogsReadOnlyAccess doesn't include "logs:CreateLogStream" but it includes "logs:Get\*"

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/iam-identity-based-access-control-cwl.html#:~:te>

#### NEW QUESTION 99

A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account.

What is the MOST secure way to provide this access?

- A. Create one IAM user in the production account
- B. Grant the appropriate permissions to the resources that are needed
- C. Share the password only with the users that need access.
- D. Create cross-account access with an IAM role in the developer account
- E. Grant the appropriate permissions to this role
- F. Allow users in the developer account to assume this role to access the production resources.
- G. Create cross-account access with an IAM user account in the production account
- H. Grant the appropriate permissions to this user account
- I. Allow users in the developer account to use this user account to access the production resources.
- J. Create cross-account access with an IAM role in the production account
- K. Grant the appropriate permissions to this role
- L. Allow users in the developer account to assume this role to access the production resources.

**Answer:** D

#### Explanation:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\\_cross-account-with-roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html)

#### NEW QUESTION 100

A security engineer needs to implement a solution to create and control the keys that a company uses for cryptographic operations. The security engineer must create symmetric keys in which the key material is generated and used within a custom key store that is backed by an AWS CloudHSM cluster.

The security engineer will use symmetric and asymmetric data key pairs for local use within applications. The security engineer also must audit the use of the keys.

How can the security engineer meet these requirements?

- A. To create the keys use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster
- B. For auditing, use Amazon Athena
- C. To create the keys use Amazon S3 and the custom key stores with the CloudHSM cluster
- D. For auditing use AWS CloudTrail.
- E. To create the keys use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster
- F. For auditing, use Amazon GuardDuty.
- G. To create the keys use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster
- H. For auditing, use AWS CloudTrail.

**Answer:** D

#### Explanation:

AWS KMS supports asymmetric KMS keys that represent a mathematically related RSA, elliptic curve (ECC), or SM2 (China Regions only) public and private key pair. These key pairs are generated in AWS KMS hardware security modules certified under the FIPS 140-2 Cryptographic Module Validation Program, except in



the China (Beijing) and China (Ningxia) Regions. The private key never leaves the AWS KMS HSMs unencrypted.  
<https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html>

#### NEW QUESTION 101

A Security Engineer has been tasked with enabling IAM Security Hub to monitor Amazon EC2 instances fix CVE in a single IAM account The Engineer has already enabled IAM Security Hub and Amazon Inspector in the IAM Management Console and has installed the Amazon Inspector agent on an EC2 instances that need to be monitored.

Which additional steps should the Security Engineer take to meet this requirement?

- A. Configure the Amazon Inspector agent to use the CVE rule package
- B. Configure the Amazon Inspector agent to use the CVE rule package Configure Security Hub to ingest from IAM Inspector by writing a custom resource policy
- C. Configure the Security Hub agent to use the CVE rule package Configure IAM Inspector to ingest from Security Hub by writing a custom resource policy
- D. Configure the Amazon Inspector agent to use the CVE rule package Install an additional Integration library Allow the Amazon Inspector agent to communicate with Security Hub

**Answer: D**

#### Explanation:

you need to configure the Amazon Inspector agent to use the CVE rule package, which is a set of rules that check for vulnerabilities and exposures on your EC2 instances<sup>5</sup>. You also need to install an additional integration library that enables communication between the Amazon Inspector agent and Security Hub<sup>6</sup>. Security Hub is a service that provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices<sup>7</sup>. The other options are either incorrect or incomplete for meeting the requirement.

#### NEW QUESTION 105

A security engineer is designing a cloud architecture to support an application. The application runs on Amazon EC2 instances and processes sensitive information, including credit card numbers.

The application will send the credit card numbers to a component that is running in an isolated environment. The component will encrypt, store, and decrypt the numbers.

The component then will issue tokens to replace the numbers in other parts of the application.

The component of the application that manages the tokenization process will be deployed on a separate set of EC2 instances. Other components of the application must not be able to store or access the credit card numbers.

Which solution will meet these requirements?

- A. Use EC2 Dedicated Instances for the tokenization component of the application.
- B. Place the EC2 instances that manage the tokenization process into a partition placement group.
- C. Create a separate VPC
- D. Deploy new EC2 instances into the separate VPC to support the data tokenization.
- E. Deploy the tokenization code onto AWS Nitro Enclaves that are hosted on EC2 instances.

**Answer: D**

#### Explanation:

AWS Nitro Enclaves are isolated and hardened virtual machines that run on EC2 instances and provide a secure environment for processing sensitive data. Nitro Enclaves have no persistent storage, interactive access, or external networking, and they can only communicate with the parent instance through a secure local channel. Nitro Enclaves also support cryptographic attestation, which allows verifying the identity and integrity of the enclave and its code. Nitro Enclaves are ideal for implementing data protection solutions such as tokenization, encryption, and key management.

Using Nitro Enclaves for the tokenization component of the application meets the requirements of isolating the sensitive data from other parts of the application, encrypting and storing the credit card numbers securely, and issuing tokens to replace the numbers. Other components of the application will not be able to access or store the credit card numbers, as they are only available within the enclave.

#### NEW QUESTION 106

A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket.

The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Configure the S3 Block Public Access feature for the AWS account.
- B. Configure the S3 Block Public Access feature for all objects that are in the bucket.
- C. Deactivate ACLs for objects that are in the bucket.
- D. Use AWS PrivateLink for Amazon S3 to access the bucket.

**Answer: D**

#### NEW QUESTION 109

A company is operating a website using Amazon CloudFront. CloudFront servers some content from Amazon S3 and other from web servers running EC2 instances behind an Application Load Balancer (ALB). Amazon DynamoDB is used as the data store. The company already uses IAM Certificate Manager (ACM) to store a public TLS certificate that can optionally secure connections between the website users and CloudFront. The company has a new requirement to enforce end-to-end encryption in transit.

Which combination of steps should the company take to meet this requirement? (Select THREE.)

- A. Update the CloudFront distribution
- B. configuring it to optionally use HTTPS when connecting to origins on Amazon S3
- C. Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB
- D. Update the CloudFront distribution to redirect HTTP connections to HTTPS
- E. Configure the web servers on the EC2 instances to listen using HTTPS using the public ACM TLS certificate Update the ALB to connect to the target group using HTTPS
- F. Update the ALB listen to listen using HTTPS using the public ACM TLS certificate
- G. Update the CloudFront distribution to connect to the HTTPS listener.
- H. Create a TLS certificate Configure the web servers on the EC2 instances to use HTTPS only with that certificate
- I. Update the ALB to connect to the target group using HTTPS.



**Answer:** BCE

**Explanation:**

To enforce end-to-end encryption in transit, the company should do the following:

- Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB. This ensures that the data is encrypted when it travels from the web servers to the data store.
- Update the CloudFront distribution to redirect HTTP requests to HTTPS. This ensures that the viewers always use HTTPS when they access the website through CloudFront.
- Update the ALB to listen using HTTPS using the public ACM TLS certificate. Update the CloudFront distribution to connect to the HTTPS listener. This ensures that the data is encrypted when it travels from CloudFront to the ALB and from the ALB to the web servers.

**NEW QUESTION 114**

A company's application team wants to replace an internal application with a new IAM architecture that consists of Amazon EC2 instances, an IAM Lambda function, and an Amazon S3 bucket in a single IAM Region. After an architecture review, the security team mandates that no application network traffic can traverse the public internet at any point. The security team already has an SCP in place for the company's organization in IAM Organizations to restrict the creation of internet gateways, NAT gateways, and egress-only gateways.

Which combination of steps should the application team take to meet these requirements? (Select THREE.)

- A. Create an S3 endpoint that has a full-access policy for the application's VPC.
- B. Create an S3 access point for the S3 bucket.
- C. Include a policy that restricts the network origin to VPCs.
- D. Launch the Lambda function.
- E. Enable the block public access configuration.
- F. Create a security group that has an outbound rule over port 443 with a destination of the S3 endpoint. Associate the security group with the EC2 instances.
- G. Create a security group that has an outbound rule over port 443 with a destination of the S3 access point. Associate the security group with the EC2 instances.
- H. Launch the Lambda function in a VPC.

**Answer:** ADF

**NEW QUESTION 118**

An ecommerce company is developing new architecture for an application release. The company needs to implement TLS for incoming traffic to the application. Traffic for the application will originate from the internet. TLS does not have to be implemented in an end-to-end configuration because the company is concerned about impacts on performance. The incoming traffic types will be HTTP and HTTPS. The application uses ports 80 and 443.

What should a security engineer do to meet these requirements?

- A. Create a public Application Load Balance.
- B. Create two listeners: one listener on port 80 and one listener on port 443. Create one target group.
- C. Create a rule to forward traffic from port 80 to the listener on port 443. Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 443.
- D. Create a public Application Load Balance.
- E. Create two listeners: one listener on port 80 and one listener on port 443. Create one target group.
- F. Create a rule to forward traffic from port 80 to the listener on port 443. Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 80.
- G. Create a public Network Load Balance.
- H. Create two listeners: one listener on port 80 and one listener on port 443. Create one target group.
- I. Create a rule to forward traffic from port 80 to the listener on port 443. Set the protocol for the listener on port 443 to TLS.
- J. Create a public Network Load Balance.
- K. Create a listener on port 443. Create one target group.
- L. Create a rule to forward traffic from port 443 to the target group.
- M. Set the protocol for the listener on port 443 to TLS.

**Answer:** A

**Explanation:**

An Application Load Balancer (ALB) is a type of load balancer that operates at the application layer (layer 7) of the OSI model. It can distribute incoming traffic based on the content of the request, such as the host header, path, or query parameters. An ALB can also terminate TLS connections and decrypt requests from clients before sending them to the targets.

To implement TLS for incoming traffic to the application, the following steps are required:

- Create a public ALB in a public subnet and register the EC2 instances as targets in a target group.
- Create two listeners for the ALB, one on port 80 for HTTP traffic and one on port 443 for HTTPS traffic.
- Create a rule for the listener on port 80 to redirect HTTP requests to HTTPS using the same host, path, and query parameters.
- Provision a public TLS certificate in AWS Certificate Manager (ACM) for the domain name of the application. ACM is a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources.
- Attach the certificate to the listener on port 443 and configure the security policy to negotiate secure connections between clients and the ALB.
- Configure the security groups for the ALB and the EC2 instances to allow inbound traffic on ports 80 and 443 from the internet and outbound traffic on any port to the EC2 instances.

This solution will meet the requirements of implementing TLS for incoming traffic without impacting performance or requiring end-to-end encryption. The ALB will handle the TLS termination and decryption, while forwarding unencrypted requests to the EC2 instances.

Verified References:

- <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>
- <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>
- <https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

**NEW QUESTION 121**

A security engineer is configuring account-based access control (ABAC) to allow only specific principals to put objects into an Amazon S3 bucket. The principals already have access to Amazon S3.

The security engineer needs to configure a bucket policy that allows principals to put objects into the S3 bucket only if the value of the Team tag on the object matches the value of the Team tag that is associated with the principal. During testing, the security engineer notices that a principal can still put objects into the S3 bucket when the tag values do not match.

Which combination of factors are causing the PutObject operation to succeed when the tag values are different? (Select TWO.)

- A. The principal's identity-based policy grants access to put objects into the S3 bucket with no conditions.
- B. The principal's identity-based policy overrides the condition because the identity-based policy contains an explicit allow.
- C. The S3 bucket's resource policy does not deny access to put objects.
- D. The S3 bucket's resource policy cannot allow actions to the principal.
- E. The bucket policy does not apply to principals in the same zone of trust.

**Answer:** AC

**Explanation:**

The correct answer is A and C.

When using ABAC, the principal's identity-based policy and the S3 bucket's resource policy are both evaluated to determine the effective permissions. If either policy grants access to the principal, the action is allowed. If either policy denies access to the principal, the action is denied. Therefore, to enforce the tag-based condition, both policies must deny access when the tag values do not match.

In this case, the principal's identity-based policy grants access to put objects into the S3 bucket with no conditions (A), which means that the policy does not check for the tag values. This policy overrides the condition in the bucket policy because an explicit allow always takes precedence over an implicit deny. The bucket policy can only allow or deny actions to the principal based on the condition, but it cannot override the identity-based policy.

The S3 bucket's resource policy does not deny access to put objects ©, which means that it also does not check for the tag values. The bucket policy can only allow or deny actions to the principal based on the condition, but it cannot override the identity-based policy.

Therefore, the combination of factors A and C are causing the PutObject operation to succeed when the tag values are different.

References:

- [Using ABAC with Amazon S3](#)
- [Bucket policy examples](#)

**NEW QUESTION 126**

A security team is using Amazon EC2 Image Builder to build a hardened AMI with forensic capabilities. An AWS Key Management Service (AWS KMS) key will encrypt the forensic AMI. EC2 Image Builder successfully installs the required patches and packages in the security team's AWS account. The security team uses a federated IAM role in the same AWS account to sign in to the AWS Management Console and attempts to launch the forensic AMI. The EC2 instance launches and immediately terminates.

What should the security team do to launch the EC2 instance successfully?

- A. Update the policy that is associated with the federated IAM role to allow the ec2:DescribeImages action for the forensic AMI.
- B. Update the policy that is associated with the federated IAM role to allow the ec2:StartInstances action in the security team's AWS account.
- C. Update the policy that is associated with the KMS key that is used to encrypt the forensic AMI.
- D. Configure the policy to allow the kms:
- E. Encrypt and kms:Decrypt actions for the federated IAM role.
- F. Update the policy that is associated with the federated IAM role to allow the kms:
- G. DescribeKey action for the KMS key that is used to encrypt the forensic AMI.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-i>

**NEW QUESTION 127**

A company that uses AWS Organizations is migrating workloads to AWS. The company's application team determines that the workloads will use Amazon EC2 instances, Amazon S3 buckets, Amazon DynamoDB tables, and Application Load Balancers. For each resource type, the company mandates that deployments must comply with the following requirements:

- All EC2 instances must be launched from approved AWS accounts.
- All DynamoDB tables must be provisioned with a standardized naming convention.
- All infrastructure that is provisioned in any accounts in the organization must be deployed by AWS CloudFormation templates.

Which combination of steps should the application team take to meet these requirements? (Select TWO.)

- A. Create CloudFormation templates in an administrator AWS account
- B. Share the stack sets with an application AWS account
- C. Restrict the template to be used specifically by the application AWS account.
- D. Create CloudFormation templates in an application AWS account
- E. Share the output with an administrator AWS account to review compliant resource
- F. Restrict output to only the administrator AWS account.
- G. Use permissions boundaries to prevent the application AWS account from provisioning specific resources unless conditions for the internal compliance requirements are met.
- H. Use SCPs to prevent the application AWS account from provisioning specific resources unless conditions for the internal compliance requirements are met.
- I. Activate AWS Config managed rules for each service in the application AWS account.

**Answer:** AD

**NEW QUESTION 130**

A company needs to use HTTPS when connecting to its web applications to meet compliance requirements. These web applications run in Amazon VPC on Amazon EC2 instances behind an Application Load Balancer (ALB). A security engineer wants to ensure that the load balancer will only accept connections over port 443, even if the ALB is mistakenly configured with an HTTP listener.

Which configuration steps should the security engineer take to accomplish this task?

- A. Create a security group with a rule that denies inbound connections from 0.0.0.0/0 on port 80. Attach this security group to the ALB to overwrite more permissive rules from the ALB's default security group.
- B. Create a network ACL that denies inbound connections from 0.0.0.0/0 on port 80. Associate the network ACL with the VPC's internet gateway.

- C. Create a network ACL that allows outbound connections to the VPC IP range on port 443 only. Associate the network ACL with the VPC's internet gateway.  
D. Create a security group with a single inbound rule that allows connections from 0.0.0.0/0 on port 443. Ensure this security group is the only one associated with the ALB

**Answer:** D

**Explanation:**

To ensure that the load balancer only accepts connections over port 443, the security engineer should do the following:

- Create a security group with a single inbound rule that allows connections from 0.0.0.0/0 on port 443. This means that the security group allows HTTPS traffic from any source IP address.
- Ensure this security group is the only one associated with the ALB. This means that the security group overrides any other rules that might allow HTTP traffic on port 80.

**NEW QUESTION 134**

A Development team has built an experimental environment to test a simple state web application. It has built an isolated VPC with a private and a public subnet. The public subnet holds only an Application Load Balancer, a NAT gateway, and an internet gateway. The private subnet holds all of the Amazon EC2 instances. There are 3 different types of servers. Each server type has its own Security Group that limits access to only required connectivity. The Security Groups have both inbound and outbound rules applied. Each subnet has both inbound and outbound network ACLs applied to limit access to only required connectivity. Which of the following should the team check if a server cannot establish an outbound connection to the internet? (Select THREE.)

- A. The route tables and the outbound rules on the appropriate private subnet security group
- B. The outbound network ACL rules on the private subnet and the Inbound network ACL rules on the public subnet
- C. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet
- D. The rules on any host-based firewall that may be applied on the Amazon EC2 instances
- E. The Security Group applied to the Application Load Balancer and NAT gateway
- F. That the 0.0.0.0 route in the private subnet route table points to the internet gateway in the public subnet

**Answer:** CEF

**Explanation:**

because these are the factors that could affect the outbound connection to the internet from a server in a private subnet. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet must allow the traffic to pass through<sup>8</sup>. The security group applied to the application load balancer and NAT gateway must also allow the traffic from the private subnet<sup>9</sup>. The 0.0.0.0/0 route in the private subnet route table must point to the NAT gateway in the public subnet, not the internet gateway<sup>10</sup>. The other options are either irrelevant or incorrect for troubleshooting the outbound connection issue.

**NEW QUESTION 137**

A company's Security Engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other AWS services. The contractor's IAM account must not be able to gain access to any other AWS service, even if the IAM account is assigned additional permissions based on IAM group membership. What should the Security Engineer do to meet these requirements?

- A. Create an Inline IAM user policy that allows for Amazon EC2 access for the contractor's IAM user.
- B. Create an IAM permissions boundary policy that allows Amazon EC2 access
- C. Associate the contractor's IAM account with the IAM permissions boundary policy.
- D. Create an IAM group with an attached policy that allows for Amazon EC2 access
- E. Associate the contractor's IAM account with the IAM group.
- F. Create an IAM role that allows for EC2 and explicitly denies all other service
- G. Instruct the contractor to always assume this role.

**Answer:** B

**NEW QUESTION 139**

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

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

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



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

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

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

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

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

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

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

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

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

**Answer: B**

**Explanation:**



<https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/>

#### NEW QUESTION 144

A company wants to receive an email notification about critical findings in AWS Security Hub. The company does not have an existing architecture that supports this functionality.

Which solution will meet the requirement?

- A. Create an AWS Lambda function to identify critical Security Hub finding
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the Lambda function
- C. Subscribe an email endpoint to the SNS topic to receive published messages.
- D. Create an Amazon Kinesis Data Firehose delivery stream
- E. Integrate the delivery stream with Amazon EventBridge
- F. Create an EventBridge rule that has a filter to detect critical Security Hub finding
- G. Configure the delivery stream to send the findings to an email address.
- H. Create an Amazon EventBridge rule to detect critical Security Hub finding
- I. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the EventBridge rule
- J. Subscribe an email endpoint to the SNS topic to receive published messages.
- K. Create an Amazon EventBridge rule to detect critical Security Hub finding
- L. Create an Amazon Simple Email Service (Amazon SES) topic as the target of the EventBridge rule
- M. Use the Amazon SES API to format the message
- N. Choose an email address to be the recipient of the message.

**Answer: C**

#### Explanation:

This solution meets the requirement of receiving an email notification about critical findings in AWS Security Hub. Amazon EventBridge is a serverless event bus that can receive events from AWS services and third-party sources, and route them to targets based on rules and filters. Amazon SNS is a fully managed pub/sub service that can send messages to various endpoints, such as email, SMS, mobile push, and HTTP. By creating an EventBridge rule that detects critical Security Hub findings and sends them to an SNS topic, the company can leverage the existing integration between these services and avoid writing custom code or managing servers. By subscribing an email endpoint to the SNS topic, the company can receive published messages in their inbox.

#### NEW QUESTION 149

An audit determined that a company's Amazon EC2 instance security group violated company policy by allowing unrestricted incoming SSH traffic. A security engineer must implement a near-real-time monitoring and alerting solution that will notify administrators of such violations.

Which solution meets these requirements with the MOST operational efficiency?

- A. Create a recurring Amazon Inspector assessment run that runs every day and uses the Network Reachability package
- B. Create an Amazon CloudWatch rule that invokes an IAM Lambda function when an assessment run starts
- C. Configure the Lambda function to retrieve and evaluate the assessment run report when it completes
- D. Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.
- E. Use the restricted-ssh IAM Config managed rule that is invoked by security group configuration changes that are not compliant
- F. Use the IAM Config remediation feature to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
- G. Configure VPC Flow Logs for the VPC
- H. and specify an Amazon CloudWatch Logs group
- I. Subscribe the CloudWatch Logs group to an IAM Lambda function that parses new log entries, detects successful connections on port 22, and publishes a notification through Amazon Simple Notification Service (Amazon SNS).
- J. Create a recurring Amazon Inspector assessment run that runs every day and uses the Security Best Practices package
- K. Create an Amazon CloudWatch rule that invokes an IAM Lambda function when an assessment run starts
- L. Configure the Lambda function to retrieve and evaluate the assessment run report when it completes
- M. Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.

**Answer: B**

#### Explanation:

The most operationally efficient solution to implement a near-real-time monitoring and alerting solution that will notify administrators of security group violations is to use the restricted-ssh AWS Config managed rule that is invoked by security group configuration changes that are not compliant. This rule checks whether security groups that are in use have inbound rules that allow unrestricted SSH traffic. If a violation is detected, AWS Config can use the remediation feature to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.

Option A is incorrect because creating a recurring Amazon Inspector assessment run that uses the Network Reachability package is not operationally efficient, as it requires setting up an assessment target and template, running the assessment every day, and invoking a Lambda function to retrieve and evaluate the assessment report. It also does not provide near-real-time monitoring and alerting, as it depends on the frequency and duration of the assessment run.

Option C is incorrect because configuring VPC Flow Logs for the VPC and specifying an Amazon CloudWatch Logs group is not operationally efficient, as it requires creating a log group and stream, enabling VPC Flow Logs for each subnet or network interface, and subscribing a Lambda function to parse and analyze the log entries. It also does not provide proactive monitoring and alerting, as it only detects successful connections on port 22 after they have occurred.

Option D is incorrect because creating a recurring Amazon Inspector assessment run that uses the Security Best Practices package is not operationally efficient, for the same reasons as option A. It also does not provide specific monitoring and alerting for security group violations, as it covers a broader range of security issues. References:

- > [AWS Config Rules]
- > [AWS Config Remediation]
- > [Amazon Inspector]
- > [VPC Flow Logs]

#### NEW QUESTION 151

A Security Engineer is working with a Product team building a web application on AWS. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML

identity provider.

Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

- A. Create a custom authorization service using AWS Lambda.
- B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
- C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
- D. Configure an Amazon Cognito identity pool to integrate with social login providers.
- E. Update DynamoDB to store the user email addresses and passwords.
- F. Update API Gateway to use a COGNITO\_USER\_POOLS authorizer.

**Answer:** BCF

**Explanation:**

The combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs are:

- B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes. This is a necessary step to federate the existing users from the SAML identity provider to the Amazon Cognito user pool, which will be used for authentication and authorization<sup>1</sup>.
- C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party. This is a necessary step to establish a trust relationship between the SAML identity provider and the Amazon Cognito user pool, which will allow the users to sign in using their existing credentials<sup>2</sup>.
- F. Update API Gateway to use a COGNITO\_USER\_POOLS authorizer. This is a necessary step to enable API Gateway to use the Amazon Cognito user pool as an authorizer for the RESTful services, which will validate the identity or access tokens that are issued by Amazon Cognito when a user signs in successfully<sup>3</sup>. The other options are incorrect because:
  - A. Creating a custom authorization service using AWS Lambda is not a necessary step, because Amazon Cognito user pools can provide built-in authorization features, such as scopes and groups, that can be used to control access to API resources<sup>4</sup>.
  - D. Configuring an Amazon Cognito identity pool to integrate with social login providers is not a necessary step, because the users already exist in a directory that is exposed through a SAML identity provider, and there is no requirement to support social login providers<sup>5</sup>.
  - E. Updating DynamoDB to store the user email addresses and passwords is not a necessary step, because the user credentials are already stored in the SAML identity provider, and there is no need to duplicate them in DynamoDB<sup>6</sup>.

References:

1: Using Tokens with User Pools 2: Adding SAML Identity Providers to a User Pool 3: Control Access to a REST API Using Amazon Cognito User Pools as Authorizer 4: API Authorization with Resource Servers and OAuth 2.0 Scopes 5: Using Identity Pools (Federated Identities) 6: Amazon DynamoDB

**NEW QUESTION 154**

A company is testing its incident response plan for compromised credentials. The company runs a database on an Amazon EC2 instance and stores the sensitive data-base credentials as a secret in AWS Secrets Manager. The secret has rotation configured with an AWS Lambda function that uses the generic rotation function template. The EC2 instance and the Lambda function are deployed in the same private subnet. The VPC has a Secrets Manager VPC endpoint. A security engineer discovers that the secret cannot rotate. The security engineer determines that the VPC endpoint is working as intended. The Amazon CloudWatch logs contain the following error:

"setSecret: Unable to log into database". Which solution will resolve this error?

- A. Use the AWS Management Console to edit the JSON structure of the secret in Secrets Manager so that the secret automatically conforms with the structure that the database requires.
- B. Ensure that the security group that is attached to the Lambda function allows outbound connections to the EC2 instance.
- C. Ensure that the security group that is attached to the EC2 instance allows inbound connections from the security group that is attached to the Lambda function.
- D. Use the Secrets Manager list-secrets command in the AWS CLI to list the secrets.
- E. Identify the database credential.
- F. Use the Secrets Manager rotate-secret command in the AWS CLI to force the immediate rotation of the secret.
- G. Add an internet gateway to the VPC.
- H. Create a NAT gateway in a public subnet.
- I. Update the VPC route tables so that traffic from the Lambda function and traffic from the EC2 instance can reach the Secrets Manager public endpoint.

**Answer:** B

**Explanation:**

This answer is correct because ensuring that the security groups allow bidirectional communication between the Lambda function and the EC2 instance will resolve the error. The error indicates that the Lambda function cannot connect to the database, which might be due to firewall rules blocking the traffic. By allowing outbound connections from the Lambda function and inbound connections to the EC2 instance, the security engineer can enable the rotation function to access and update the database credentials.

**NEW QUESTION 157**

A company is designing a new application stack. The design includes web servers and backend servers that are hosted on Amazon EC2 instances. The design also includes an Amazon Aurora MySQL DB cluster.

The EC2 instances are in an Auto Scaling group that uses launch templates. The EC2 instances for the web layer and the backend layer are backed by Amazon Elastic Block Store (Amazon EBS) volumes. No layers are encrypted at rest. A security engineer needs to implement encryption at rest.

Which combination of steps will meet these requirements? (Select TWO.)

- A. Modify EBS default encryption settings in the target AWS Region to enable encryption.
- B. Use an Auto Scaling group instance refresh.
- C. Modify the launch templates for the web layer and the backend layer to add AWS Certificate Manager (ACM) encryption for the attached EBS volume.
- D. Use an Auto Scaling group instance refresh.
- E. Create a new AWS Key Management Service (AWS KMS) encrypted DB cluster from a snapshot of the existing DB cluster.
- F. Apply AWS Key Management Service (AWS KMS) encryption to the existing DB cluster.
- G. Apply AWS Certificate Manager (ACM) encryption to the existing DB cluster.

**Answer:** AC

**Explanation:**

<https://docs.aws.amazon.com/AuroraUserGuide/Overview.Encryption.html> <https://aws.amazon.com/premiumsupport/knowledge-center/ebs-automatic-encryption/>

To implement encryption at rest for both the EC2 instances and the Aurora DB cluster, the following steps are required:

- For the EC2 instances, modify the EBS default encryption settings in the target AWS Region to enable encryption. This will ensure that any new EBS volumes created in that Region are encrypted by default using an AWS managed key. Alternatively, you can specify a customer managed key when creating new EBS volumes. For more information, see Amazon EBS encryption.
  - Use an Auto Scaling group instance refresh to replace the existing EC2 instances with new ones that have encrypted EBS volumes attached. An instance refresh is a feature that helps you update all instances in an Auto Scaling group in a rolling fashion without the need to manage the instance replacement process manually. For more information, see Replacing Auto Scaling instances based on an instance refresh.
  - For the Aurora DB cluster, create a new AWS Key Management Service (AWS KMS) encrypted DB cluster from a snapshot of the existing DB cluster. You can use either an AWS managed key or a customer managed key to encrypt the new DB cluster. You cannot enable or disable encryption for an existing DB cluster, so you have to create a new one from a snapshot. For more information, see Encrypting Amazon Aurora resources.
- The other options are incorrect because they either do not enable encryption at rest for the resources (B, D), or they use the wrong service for encryption (E).

Verified References:

- <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>
- <https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-instance-refresh.html>
- <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.Encryption.html>

#### NEW QUESTION 159

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:

The following may be causing the problem for the Auditor:

- A. The external ID used by the Auditor is missing or incorrect. This is a possible cause, because the external ID is a unique identifier that is used to establish a trust relationship between the accounts. The external ID must match the one that is specified in the role's trust policy in the destination account<sup>1</sup>.
- C. The Auditor has not been granted sts:AssumeRole for the role in the destination account. This is a possible cause, because sts:AssumeRole is the API action that allows the Auditor to assume the cross-account role and obtain temporary credentials. The Auditor must have an IAM policy that allows them to call sts:AssumeRole for the role ARN in the destination account<sup>2</sup>.
- F. The role ARN used by the Auditor is missing or incorrect. This is a possible cause, because the role ARN is the Amazon Resource Name of the cross-account role that the Auditor wants to assume. The role ARN must be valid and exist in the destination account<sup>3</sup>.

#### NEW QUESTION 162

A company is migrating one of its legacy systems from an on-premises data center to AWS. The application server will run on AWS, but the database must remain in the on-premises data center for compliance reasons. The database is sensitive to network latency. Additionally, the data that travels between the on-premises data center and AWS must have IPsec encryption. Which combination of AWS solutions will meet these requirements? (Choose two.)

- A. AWS Site-to-Site VPN
- B. AWS Direct Connect
- C. AWS VPN CloudHub
- D. VPC peering
- E. NAT gateway

**Answer:** AB

#### Explanation:

The correct combination of AWS solutions that will meet these requirements is A. AWS Site-to-Site VPN and B. AWS Direct Connect.

- \* A. AWS Site-to-Site VPN is a service that allows you to securely connect your on-premises data center to your AWS VPC over the internet using IPsec encryption. This solution meets the requirement of encrypting the data in transit between the on-premises data center and AWS.
- \* B. AWS Direct Connect is a service that allows you to establish a dedicated network connection between your on-premises data center and your AWS VPC. This solution meets the requirement of reducing network latency between the on-premises data center and AWS.
- \* C. AWS VPN CloudHub is a service that allows you to connect multiple VPN connections from different locations to the same virtual private gateway in your AWS VPC. This solution is not relevant for this scenario, as there is only one on-premises data center involved.
- \* D. VPC peering is a service that allows you to connect two or more VPCs in the same or different regions using private IP addresses. This solution does not meet the requirement of connecting an on-premises data center to AWS, as it only works for VPCs.
- \* E. NAT gateway is a service that allows you to enable internet access for instances in a private subnet in your AWS VPC. This solution does not meet the requirement of connecting an on-premises data center to AWS, as it only works for outbound traffic from your VPC.

#### NEW QUESTION 165

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### SCS-C02 Practice Exam Features:

- \* SCS-C02 Questions and Answers Updated Frequently
- \* SCS-C02 Practice Questions Verified by Expert Senior Certified Staff
- \* SCS-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SCS-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SCS-C02 Practice Test Here](#)**