



# Amazon-Web-Services

## Exam Questions SCS-C02

AWS Certified Security - Specialty

**NEW QUESTION 1**

A security engineer needs to create an Amazon S3 bucket policy to grant least privilege read access to IAM user accounts that are named User=1, User2. and User3. These IAM user accounts are members of the AuthorizedPeople IAM group. The security engineer drafts the following S3 bucket policy:

```
{
  "Version": "2012-10-17",
  "Id": "AuthorizedPeoplePolicy",
  "Statement": [
    {
      "Sid": "Actions-Authorized-People",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::authorized-people-bucket/*"
    }
  ]
}
```

When the security engineer tries to add the policy to the S3 bucket, the following error message appears: "Missing required field Principal." The security engineer is adding a Principal element to the policy. The addition must provide read access to only User1. User2, and User3. Which solution meets these requirements?

A)

```
"Principal": {
  "AWS": [
    "arn:aws:iam::1234567890:user/User1",
    "arn:aws:iam::1234567890:user/User2",
    "arn:aws:iam::1234567890:user/User3"
  ]
}
```

B)

```
"Principal": {
  "AWS": [
    "arn:aws:iam::1234567890:root"
  ]
}
```

C)

```
"Principal": {
  "AWS": [
    "*"
  ]
}
```

D)

```
"Principal": {
  "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"
}
```

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

**Answer: A**

**NEW QUESTION 2**

A company hosts an end user application on AWS. Currently the company deploys the application on Amazon EC2 instances behind an Elastic Load Balancer. The company wants to configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances.

Which solution will meet this requirement with the LEAST operational effort?

- A. Use Amazon issued AWS Certificate Manager (ACM) certificates on the EC2 instances and the Elastic Load Balancer to configure end-to-end encryption
- B. Import a third-party SSL certificate to AWS Certificate Manager (ACM). Install the third-party certificate on the EC2 instances. Associate the ACM imported third-party certificate with the Elastic Load Balancer.
- C. Deploy AWS CloudHSM. Import a third-party certificate. Configure the EC2 instances and the Elastic Load Balancer to use the CloudHSM imported certificate.
- D. Import a third-party certificate bundle to AWS Certificate Manager (ACM). Install the third-party certificate on the EC2 instances. Associate the ACM imported third-party certificate with the Elastic Load Balancer.

**Answer: A**

**Explanation:**

To configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances with the least operational effort, the most appropriate solution would be to use Amazon issued AWS Certificate Manager (ACM) certificates on the EC2 instances and the Elastic Load Balancer to configure end-to-end encryption.

AWS Certificate Manager - Amazon Web Services : Elastic Load Balancing - Amazon Web

Services : Amazon Elastic Compute Cloud - Amazon Web Services : AWS Certificate Manager - Amazon Web Services

**NEW QUESTION 3**

A company hosts a public website on an Amazon EC2 instance. HTTPS traffic must be able to access the website. The company uses SSH for management of

the web server.

The website is on the subnet 10.0.1.0/24. The management subnet is 192.168.100.0/24. A security engineer must create a security group for the EC2 instance. Which combination of steps should the security engineer take to meet these requirements in the MOST secure manner? (Select TWO.)

- A. Allow port 22 from source 0.0.0.0/0.
- B. Allow port 443 from source 0.0.0.0/0.
- C. Allow port 22 from 192.168.100.0/24.
- D. Allow port 22 from 10.0.1.0/24.
- E. Allow port 443 from 10.0.1.0/24.

**Answer:** BC

**Explanation:**

The correct answer is B and C.

\* B. Allow port 443 from source 0.0.0.0/0.

This is correct because port 443 is used for HTTPS traffic, which must be able to access the website from any source IP address.

\* C. Allow port 22 from 192.168.100.0/24.

This is correct because port 22 is used for SSH, which is the management protocol for the web server. The management subnet is 192.168.100.0/24, so only this subnet should be allowed to access port 22.

\* A. Allow port 22 from source 0.0.0.0/0.

This is incorrect because it would allow anyone to access port 22, which is a security risk. SSH should be restricted to the management subnet only.

\* D. Allow port 22 from 10.0.1.0/24.

This is incorrect because it would allow the website subnet to access port 22, which is unnecessary and a security risk. SSH should be restricted to the management subnet only.

\* E. Allow port 443 from 10.0.1.0/24.

This is incorrect because it would limit the HTTPS traffic to the website subnet only, which defeats the purpose of having a public website.

**NEW QUESTION 4**

A company is implementing new compliance requirements to meet customer needs. According to the new requirements the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster. Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an AWS Config managed rule to detect unencrypted ROS storag
- B. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
- C. Configure the Lambda function to delete the unencrypted resource.
- D. Create an AWS Config managed rule to detect unencrypted RDS storag
- E. Configure a manual remediation action to invoke an AWS Lambda functio
- F. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- G. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
- H. Configure the Lambda function to delete the unencrypted resource.
- I. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster
- J. Configure the rule to invoke an AWS Lambda functio
- K. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/config/latest/developerguide/rds-storage-encrypted.html>

**NEW QUESTION 5**

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 6**

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 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 designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS Single Sign-On (AWS SSO). The company must implement a solution so that the development teams can use only specific AWS Regions and so that each AWS account allows access to only specific AWS services.

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

- A. Use AWS SSO to set up service-linked roles with IAM policy statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
- B. Deactivate AWS Security Token Service (AWS STS) in Regions that the developers are not allowed to use.
- C. Create SCPs that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
- D. For each AWS account, create tailored identity-based policies for AWS SS
- E. Use statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

**Answer:** C

**Explanation:**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_syntax.html#scp-eleme](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_syntax.html#scp-eleme)

**NEW QUESTION 9**

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 10

A company uses AWS Organizations to manage a small number of AWS accounts. However, the company plans to add 1 000 more accounts soon. The company allows only a centralized security team to create IAM roles for all AWS accounts and teams. Application teams submit requests for IAM roles to the security team. The security team has a backlog of IAM role requests and cannot review and provision the IAM roles quickly.

The security team must create a process that will allow application teams to provision their own IAM roles. The process must also limit the scope of IAM roles and prevent privilege escalation.

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

- A. Create an IAM group for each application team
- B. Associate policies with each IAM group
- C. Provision IAM users for each application team member
- D. Add the new IAM users to the appropriate IAM group by using role-based access control (RBAC).
- E. Delegate application team leads to provision IAM roles for each team
- F. Conduct a quarterly review of the IAM roles the team leads have provisioned
- G. Ensure that the application team leads have the appropriate training to review IAM roles.
- H. Put each AWS account in its own OU
- I. Add an SCP to each OU to grant access to only the AWS services that the teams plan to use
- J. Include conditions in the AWS account of each team.
- K. Create an SCP and a permissions boundary for IAM role
- L. Add the SCP to the root OU so that only roles that have the permissions boundary attached can create any new IAM roles.

**Answer:** D

#### Explanation:

To create a process that will allow application teams to provision their own IAM roles, while limiting the scope of IAM roles and preventing privilege escalation, the following steps are required:

➤ Create a service control policy (SCP) that defines the maximum permissions that can be granted to any IAM role in the organization. An SCP is a type of policy that you can use with AWS Organizations to manage permissions for all accounts in your organization. SCPs restrict permissions for entities in member accounts, including each AWS account root user, IAM users, and roles. For more information, see [Service control policies overview](#).

➤ Create a permissions boundary for IAM roles that matches the SCP. A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. A permissions boundary allows an entity to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. For more information, see [Permissions boundaries for IAM entities](#).

➤ Add the SCP to the root organizational unit (OU) so that it applies to all accounts in the organization.

This will ensure that no IAM role can exceed the permissions defined by the SCP, regardless of how it is created or modified.

➤ Instruct the application teams to attach the permissions boundary to any IAM role they create. This will prevent them from creating IAM roles that can escalate their own privileges or access resources they are not authorized to access.

This solution will meet the requirements with the least operational overhead, as it leverages AWS Organizations and IAM features to delegate and limit IAM role creation without requiring manual reviews or approvals.

The other options are incorrect because they either do not allow application teams to provision their own IAM roles (A), do not limit the scope of IAM roles or prevent privilege escalation (B), or do not take advantage of managed services whenever possible ©.

Verified References:

➤ [https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_boundaries.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html)

#### NEW QUESTION 11

Your CTO is very worried about the security of your IAM account. How best can you prevent hackers from completely hijacking your account?  
 Please select:

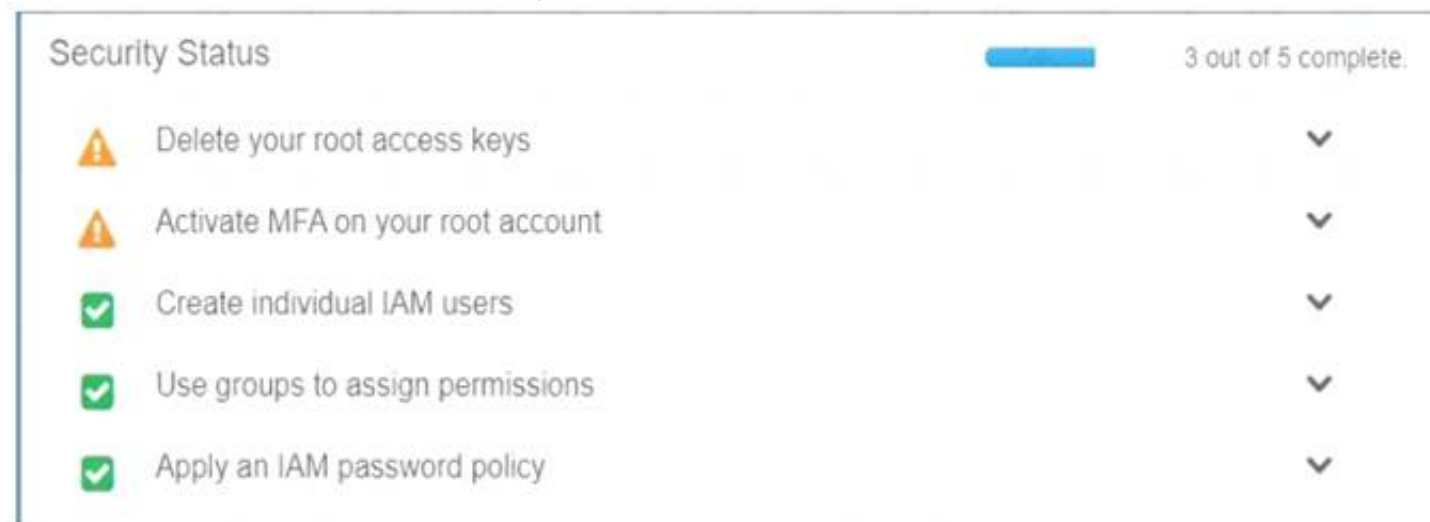
- A. Use short but complex password on the root account and any administrators.
- B. Use IAM IAM Geo-Lock and disallow anyone from logging in except for in your city.
- C. Use MFA on all users and accounts, especially on the root account.
- D. Don't write down or remember the root account password after creating the IAM account.

**Answer: C**

#### Explanation:

Multi-factor authentication can add one more layer of security to your IAM account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account

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



Option A is invalid because you need to have a good password policy Option B is invalid because there is no IAM Geo-Lock Option D is invalid because this is not a recommended practices For more information on MFA, please visit the below URL

[http://docs.IAM.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_mfa.html](http://docs.IAM.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html)

The correct answer is: Use MFA on all users and accounts, especially on the root account. Submit your Feedback/Queries to our Experts

#### NEW QUESTION 14

A security engineer is designing an IAM policy to protect AWS API operations. The policy must enforce multi-factor authentication (MFA) for IAM users to access certain services in the AWS production account. Each session must remain valid for only 2 hours. The current version of the IAM policy is as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Resource": ["*"]
  }]
}
```

Which combination of conditions must the security engineer add to the IAM policy to meet these requirements? (Select TWO.)

- A. "Bool" : "aws : Multi FactorAuthPresent": "true" }
- B. "B001" : "aws : MultiFactorAuthPresent": "false" }
- C. "NumericLessThan" : { "aws : Multi FactorAuthAge" : "7200" }
- D. "NumericGreaterThan" : { "aws : MultiFactorAuthAge" : "7200" }
- E. "NumericLessThan" : { "MaxSessionDuration" : "7200" }

**Answer: AC**

#### Explanation:

The correct combination of conditions to add to the IAM policy is A and C. These conditions will ensure that IAM users must use MFA to access certain services in the AWS production account, and that each session will expire after 2 hours.

➤ Option A: "Bool" : { "aws:MultiFactorAuthPresent" : "true" } is a valid condition that checks if the principal (the IAM user) has authenticated with MFA before

making the request. This condition will enforce MFA for the IAM users to access the specified services. This condition key is supported by all AWS services that support IAM policies1.

➤ Option B: "Bool" : { "aws:MultiFactorAuthPresent" : "false" } is the opposite of option A. This condition will allow access only if the principal has not authenticated with MFA, which is not the desired requirement. This condition key is supported by all AWS services that support IAM policies1.

➤ Option C: "NumericLessThan" : { "aws:MultiFactorAuthAge" : "7200" } is a valid condition that checks if the time since the principal authenticated with MFA is less than 7200 seconds (2 hours). This condition will enforce the session duration limit for the IAM users. This condition key is supported by all AWS services that support IAM policies1.

➤ Option D: "NumericGreaterThan" : { "aws:MultiFactorAuthAge" : "7200" } is the opposite of option C. This condition will allow access only if the time since the principal authenticated with MFA is more than 7200 seconds (2 hours), which is not the desired requirement. This condition key is supported by all AWS services that support IAM policies1.

➤ Option E: "NumericLessThan" : { "MaxSessionDuration" : "7200" } is not a valid condition key.

MaxSessionDuration is a property of an IAM role, not a condition key. It specifies the maximum session duration (in seconds) for the role, which can be between 3600 and 43200 seconds (1 to 12 hours). This property can be set when creating or modifying a role, but it cannot be used as a condition in a policy2.

#### NEW QUESTION 15

A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised. The instance was serving up malware. The analysis of the instance showed that the instance was compromised 35 days ago.

A security engineer must implement a continuous monitoring solution that automatically notifies the company's security team about compromised instances through an email distribution list for high severity findings. The security engineer must implement the solution as soon as possible.

Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

- A. Enable AWS Security Hub in the AWS account.
- B. Enable Amazon GuardDuty in the AWS account.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Subscribe the security team's email distribution list to the topic.
- E. Create an Amazon Simple Queue Service (Amazon SQS) queue.
- F. Subscribe the security team's email distribution list to the queue.
- G. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for GuardDuty findings of high severity.
- H. Configure the rule to publish a message to the topic.
- I. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for Security Hub findings of high severity.
- J. Configure the rule to publish a message to the queue.

**Answer:** BCE

#### NEW QUESTION 17

A company is planning to use Amazon Elastic File System (Amazon EFS) with its on-premises servers. The company has an existing IAM Direct Connect connection established between its on-premises data center and an IAM Region. A security policy states that the company's on-premises firewall should only have specific IP addresses added to the allow list and not a CIDR range. The company also wants to restrict access so that only certain data center-based servers have access to Amazon EFS.

How should a security engineer implement this solution?

- A. Add the file-system-id efs IAM-region amazonIAM.com URL to the allow list for the data center firewall. Install the IAM CLI on the data center-based servers to mount the EFS file system. In the EFS security group, add the data center IP range to the allow list. Mount the EFS using the EFS file system name.
- B. Assign an Elastic IP address to Amazon EFS and add the Elastic IP address to the allow list for the data center firewall. Install the IAM CLI on the data center-based servers to mount the EFS file system. In the EFS security group, add the IP addresses of the data center servers to the allow list. Mount the EFS using the Elastic IP address.
- C. Add the EFS file system mount target IP addresses to the allow list for the data center firewall. In the EFS security group, add the data center server IP addresses to the allow list. Use the Linux terminal to mount the EFS file system using the IP address of one of the mount targets.
- D. Assign a static range of IP addresses for the EFS file system by contacting IAM Support. In the EFS security group, add the data center server IP addresses to the allow list. Use the Linux terminal to mount the EFS file system using one of the static IP addresses.

**Answer:** B

#### Explanation:

To implement the solution, the security engineer should do the following:

- Assign an Elastic IP address to Amazon EFS and add the Elastic IP address to the allow list for the data center firewall. This allows the security engineer to use a specific IP address for the EFS file system that can be added to the firewall rules, instead of a CIDR range or a URL.
- Install the AWS CLI on the data center-based servers to mount the EFS file system. This allows the security engineer to use the mount helper provided by AWS CLI to mount the EFS file system with encryption in transit.
- In the EFS security group, add the IP addresses of the data center servers to the allow list. This allows the security engineer to restrict access to the EFS file system to only certain data center-based servers.
- Mount the EFS using the Elastic IP address. This allows the security engineer to use the Elastic IP address as the DNS name for mounting the EFS file system.

#### NEW QUESTION 22

Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets.

Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC. These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table.

The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.

How will the security engineer be able to comply with these requirements?

- A. Remove the existing NAT gateway.
- B. Create a new NAT gateway that only the application server subnets can use.
- C. Configure the DB instance's inbound network ACL to deny traffic from the security group ID of the NAT gateway.



- D. Modify the route tables of the DB instance subnets to remove the default route to the NAT gateway.
- E. Configure the route table of the NAT gateway to deny connections to the DB instance subnets.

**Answer:** C

**Explanation:**

Each subnet has a route table, so modify the routing associated with DB instance subnets to prevent internet access.

**NEW QUESTION 26**

A company uses an external identity provider to allow federation into different IAM accounts. A security engineer for the company needs to identify the federated user that terminated a production Amazon EC2 instance a week ago.

What is the FASTEST way for the security engineer to identify the federated user?

- A. Review the IAM CloudTrail event history logs in an Amazon S3 bucket and look for the TerminateInstances event to identify the federated user from the role session name.
- B. Filter the IAM CloudTrail event history for the TerminateInstances event and identify the assumed IAM role.
- C. Review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username.
- D. Search the IAM CloudTrail logs for the TerminateInstances event and note the event time.
- E. Review the IAM Access Advisor tab for all federated roles.
- F. The last accessed time should match the time when the instance was terminated.
- G. Use Amazon Athena to run a SQL query on the IAM CloudTrail logs stored in an Amazon S3 bucket and filter on the TerminateInstances event.
- H. Identify the corresponding role and run another query to filter the AssumeRoleWithWebIdentity event for the user name.

**Answer:** B

**Explanation:**

The fastest way to identify the federated user who terminated a production Amazon EC2 instance is to filter the IAM CloudTrail event history for the TerminateInstances event and identify the assumed IAM role. Then, review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username. This method does not require any additional tools or queries, and it directly links the IAM role with the federated user.

Option A is incorrect because the role session name may not be the same as the federated user name, and it may not be unique or descriptive enough to identify the user.

Option C is incorrect because the IAM Access Advisor tab only shows when a role was last accessed, not by whom or for what purpose. It also does not show the specific time of access, only the date.

Option D is incorrect because using Amazon Athena to run SQL queries on the IAM CloudTrail logs is not the fastest way to identify the federated user, as it requires creating a table schema and running multiple queries. It also assumes that the federation is done using web identity providers, not SAML providers, as indicated by the AssumeRoleWithWebIdentity event.

References:

- > [AWS Identity and Access Management](#)
- > [Logging AWS STS API Calls with AWS CloudTrail](#)
- > [\[Using Amazon Athena to Query S3 Data for CloudTrail Analysis\]](#)

**NEW QUESTION 31**

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

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

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

**Answer:** CE

**Explanation:**

AWS Secrets Manager is a service that helps you manage, retrieve, and rotate secrets such as database credentials, API keys, and other sensitive information. By configuring automatic rotation of credentials in AWS Secrets Manager, you can ensure that your secrets are changed regularly and securely, without requiring manual intervention or application downtime. You can also specify the rotation frequency and the rotation function that performs the logic of changing the credentials on the database and updating the secret in Secrets Manager<sup>1</sup>.

\* E. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotated. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

By configuring the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials, you can avoid hard-coding the credentials in your application code or configuration files. This way, your application can dynamically obtain the latest credentials from Secrets Manager whenever the password is rotated, without needing to restart or redeploy the application. To enable this, you need to grant permission to the instance role associated with the EC2 instance to access Secrets Manager using IAM policies<sup>2</sup>. You can also use the AWS SDK for Java to integrate your application with Secrets Manager<sup>3</sup>.

**NEW QUESTION 34**

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

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

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



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

**Answer:** B

#### NEW QUESTION 36

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

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

**Answer:** C

#### Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#eni-basics> Source/destination checking "You must disable source/destination checks if the instance runs services such as network address translation, routing, or firewalls."

The correct answer is C. Disable the Network Source/Destination check on the security appliance's elastic network interface.

This answer is correct because disabling the Network Source/Destination check allows the virtual security appliance to route traffic that is not addressed to or from itself. By default, this check is enabled on all EC2 instances, and it prevents them from forwarding traffic that does not match their own IP or MAC addresses.

However, for a virtual security appliance that acts as a router or a firewall, this check needs to be disabled, otherwise it will drop the traffic that it is supposed to route<sup>12</sup>.

The other options are incorrect because:

- A. Disabling network ACLs is not a solution, because network ACLs are optional layers of security for the subnets in a VPC. They can be used to allow or deny traffic based on IP addresses and ports, but they do not affect the routing behavior of the virtual security appliance<sup>3</sup>.
- B. Configuring the security appliance's elastic network interface for promiscuous mode is not a solution, because promiscuous mode is a mode for a network interface that causes it to pass all traffic it receives to the CPU, rather than passing only the frames that it is programmed to receive. Promiscuous mode is normally used for packet sniffing or monitoring, but it does not enable the network interface to route traffic<sup>4</sup>.
- D. Placing the security appliance in the public subnet with the internet gateway is not a solution, because it does not address the routing issue of the virtual security appliance. The security appliance can be placed in either a public or a private subnet, depending on the network design and security requirements, but it still needs to have the Network Source/Destination check disabled to route traffic properly<sup>5</sup>.

References:

1: Enabling or disabling source/destination checks - Amazon Elastic Compute Cloud 2: Virtual security appliance - Wikipedia 3: Network ACLs - Amazon Virtual Private Cloud 4: Promiscuous mode - Wikipedia 5: NAT instances - Amazon Virtual Private Cloud

#### NEW QUESTION 40

A company's public Application Load Balancer (ALB) recently experienced a DDoS attack. To mitigate this issue, the company deployed Amazon CloudFront in front of the ALB so that users would not directly access the Amazon EC2 instances behind the ALB.

The company discovers that some traffic is still coming directly into the ALB and is still being handled by the EC2 instances.

Which combination of steps should the company take to ensure that the EC2 instances will receive traffic only from CloudFront? (Choose two.)

- A. Configure CloudFront to add a cache key policy to allow a custom HTTP header that CloudFront sends to the ALB.
- B. Configure CloudFront to add a custom: HTTP header to requests that CloudFront sends to the ALB.
- C. Configure the ALB to forward only requests that contain the custom HTTP header.
- D. Configure the ALB and CloudFront to use the X-Forwarded-For header to check client IP addresses.
- E. Configure the ALB and CloudFront to use the same X.509 certificate that is generated by AWS Certificate Manager (ACM).

**Answer:** BC

#### Explanation:

To prevent users from directly accessing an Application Load Balancer and allow access only through CloudFront, complete these high-level steps: Configure CloudFront to add a custom HTTP header to requests that it sends to the Application Load Balancer. Configure the Application Load Balancer to only forward requests that contain the custom HTTP header. (Optional) Require HTTPS to improve the security of this solution.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html>

#### NEW QUESTION 41

A company needs to follow security best practices to deploy resources from an AWS CloudFormation template. The CloudFormation template must be able to configure sensitive database credentials.

The company already uses AWS Key Management Service (AWS KMS) and AWS Secrets Manager. Which solution will meet the requirements?

- A. Use a dynamic reference in the CloudFormation template to reference the database credentials in Secrets Manager.
- B. Use a parameter in the CloudFormation template to reference the database credential
- C. Encrypt the CloudFormation template by using AWS KMS.
- D. Use a SecureString parameter in the CloudFormation template to reference the database credentials in Secrets Manager.
- E. Use a SecureString parameter in the CloudFormation template to reference an encrypted value in AWS KMS

**Answer:** A

#### Explanation:

- Option A: This option meets the requirements of following security best practices and configuring sensitive database credentials in the CloudFormation template. A dynamic reference is a way to specify external values that are stored and managed in other services, such as Secrets Manager, in the stack templates<sup>1</sup>. When using a dynamic reference, CloudFormation retrieves the value of the specified reference when necessary during stack and change set

operations1. Dynamic references can be used for certain resources that support them, such as AWS::RDS::DBInstance1. By using a dynamic reference to reference the database credentials in Secrets Manager, the company can leverage the existing integration between these services and avoid hardcoding the secret information in the template. Secrets Manager is a service that helps you protect secrets needed to access your applications, services, and IT resources2. Secrets Manager enables you to rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle2.

#### NEW QUESTION 46

A company's Security Team received an email notification from the Amazon EC2 Abuse team that one or more of the company's Amazon EC2 instances may have been compromised

Which combination of actions should the Security team take to respond to (be current modem? (Select TWO.)

- A. Open a support case with the IAM Security team and ask them to remove the malicious code from the affected instance
- B. Respond to the notification and list the actions that have been taken to address the incident
- C. Delete all IAM users and resources in the account
- D. Detach the internet gateway from the VPC remove aft rules that contain 0.0.0.0V0 from the security groups, and create a NACL rule to deny all traffic Inbound from the internet
- E. Delete the identified compromised instances and delete any associated resources that the Security team did not create.

**Answer:** DE

#### Explanation:

these are the recommended actions to take when you receive an abuse notice from AWS8. You should review the abuse notice to see what content or activity was reported and detach the internet gateway from the VPC to isolate the affected instances from the internet. You should also remove any rules that allow inbound traffic from 0.0.0.0/0 from the security groups and create a network access control list (NACL) rule to deny all traffic inbound from the internet. You should then delete the compromised instances and any associated resources that you did not create. The other options are either inappropriate or unnecessary for responding to the abuse notice.

#### NEW QUESTION 50

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 51

A company is using IAM Organizations to develop a multi-account secure networking strategy. The company plans to use separate centrally managed accounts for shared services, auditing, and security inspection. The company plans to provide dozens of additional accounts to application owners for production and development environments.

Company security policy requires that all internet traffic be routed through a centrally managed security inspection layer in the security inspection account. A security engineer must recommend a solution that minimizes administrative overhead and complexity.

Which solution meets these requirements?

- A. Use IAM Control Towe
- B. Modify the default Account Factory networking template to automatically associate new accounts with a centrally managed VPC through a VPC peering connection and to create a default route to the VPC peer in the default route tabl
- C. Create an SCP that denies the CreateInternetGateway actio
- D. Attach the SCP to all accounts except the security inspection account.
- E. Create a centrally managed VPC in the security inspection accoun
- F. Establish VPC peering connections between the security inspection account and other account
- G. Instruct account owners to create default routes in their account route tables that point to the VPC pee
- H. Create an SCP that denies theAttach InternetGateway actio
- I. Attach the SCP to all accounts except the security inspection account.
- J. Use IAM Control Towe
- K. Modify the default Account Factory networking template to automatically associate new accounts with a centrally managed transitgateway and to create a default route to the transit gateway in the default route tabl
- L. Create an SCP that denies the AttachInternetGateway actio
- M. Attach the SCP to all accounts except the security inspection account.
- N. Enable IAM Resource Access Manager (IAM RAM) for IAM Organization

- O. Create a shared transit gateway, and make it available by using an IAM RAM resource shar
- P. Create an SCP that denies the CreateInternetGateway actio
- Q. Attach the SCP to all accounts except the security inspection accoun
- R. Create routes in the route tables of all accounts that point to the shared transit gateway.

**Answer: C**

#### NEW QUESTION 52

A company needs to store multiple years of financial records. The company wants to use Amazon S3 to store copies of these documents. The company must implement a solution to prevent the documents from being edited, replaced, or deleted for 7 years after the documents are stored in Amazon S3. The solution must also encrypt the documents at rest.

A security engineer creates a new S3 bucket to store the documents. What should the security engineer do next to meet these requirements?

- A. Configure S3 server-side encryptio
- B. Create an S3 bucket policy that has an explicit deny rule for all users for s3:DeleteObject and s3:PutObject API call
- C. Configure S3 Object Lock to use governance mode with a retention period of 7 years.
- D. Configure S3 server-side encryptio
- E. Configure S3 Versioning on the S3 bucke
- F. Configure S3 ObjectLock to use compliance mode with a retention period of 7 years.
- G. Configure S3 Versionin
- H. Configure S3 Intelligent-Tiering on the S3 bucket to move the documents to S3 Glacier Deep Archive storag
- I. Use S3 server-side encryption immediatel
- J. Expire the objects after 7 years.
- K. Set up S3 Event Notifications and use S3 server-side encryptio
- L. Configure S3 Event Notifications to target an AWS Lambda function that will review any S3 API call to the S3 bucket and deny the s3:DeleteObject and s3:PutObject API call
- M. Remove the S3 event notification after 7 years.

**Answer: B**

#### NEW QUESTION 56

A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket direct. Which solution will meet these requirements?

- A. Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.
- B. Create an origin access identity (OAI). Associate the OAI with the CloudFront distributio
- C. Configure the S3 bucket permissions so that only the OAI can access the files in the S3 bucket.
- D. Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.
- E. Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

**Answer: B**

#### NEW QUESTION 59

A development team is using an IAM Key Management Service (IAM KMS) CMK to try to encrypt and decrypt a secure string parameter from IAM Systems Manager Parameter Store. However, the development team receives an error message on each attempt. Which issues that are related to the CMK could be reasons for the error? (Select TWO.)

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

**Answer: AD**

#### NEW QUESTION 62

A company's IAM account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3. As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level? Please select:

- A. Create a new role and add each user to the IAM role
- B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
- C. Create a policy and apply it to multiple users using a JSON script
- D. Create an S3 bucket policy with unlimited access which includes each user's IAM account ID

**Answer: B**

#### Explanation:

Option A is incorrect since you don't add a user to the IAM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach

An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group

For more information on IAM Groups, just browse to the below URL: [https://docs.IAM.amazon.com/IAM/latest/UserGuide/id\\_eroups.html](https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html)

The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 65

A company is using IAM Organizations. The company wants to restrict IAM usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new IAM accounts under the development OU.

- ☐ A. Include the following SCP on the development OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```

- ☐ B. Include the following SCP on the development account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```



- ☐ C. Include the following SCP on the development OU

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```

- ☐ D. Include the following SCP on the development OU

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Allow",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "us-east-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```

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

**Answer: A**

#### NEW QUESTION 66

A company is running its workloads in a single AWS Region and uses AWS Organizations. A security engineer must implement a solution to prevent users from launching resources in other Regions.

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

- A. Create an IAM policy that has an aws RequestedRegion condition that allows actions only in the designated Region Attach the policy to all users.  
 B. Create an IAM policy that has an aws RequestedRegion condition that denies actions that are not in the designated Region Attach the policy to the AWS account in AWS Organizations.  
 C. Create an IAM policy that has an aws RequestedRegion condition that allows the desired actions Attach the policy only to the users who are in the designated Region.  
 D. Create an SCP that has an aws RequestedRegion condition that denies actions that are not in the designated Region.  
 E. Attach the SCP to the AWS account in AWS Organizations.

**Answer:** D

**Explanation:**

Although you can use a IAM policy to prevent users launching resources in other regions. The best practice is to use SCP when using AWS organizations.  
[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_general.htm](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.htm)

**NEW QUESTION 70**

A business stores website images in an Amazon S3 bucket. The firm serves the photos to end users through Amazon CloudFront. The firm learned lately that the photographs are being accessible from nations in which it does not have a distribution license.

Which steps should the business take to safeguard the photographs and restrict their distribution? (Select two.)

- A. Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI).
- B. Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.
- C. Add a CloudFront geo restriction deny list of countries where the company lacks a license.
- D. Update the S3 bucket policy with a deny list of countries where the company lacks a license.
- E. Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

**Answer:** AC

**Explanation:**

For Enable Geo-Restriction, choose Yes. For Restriction Type, choose Whitelist to allow access to certain countries, or choose Blacklist to block access from certain countries. <https://IAM.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/>

**NEW QUESTION 74**

A company is deploying an Amazon EC2-based application. The application will include a custom health-checking component that produces health status data in JSON format. A Security Engineer must

implement a secure solution to monitor application availability in near-real time by analyzing the health status data.

Which approach should the Security Engineer use?

- A. Use Amazon CloudWatch monitoring to capture Amazon EC2 and networking metrics Visualizemetrics using Amazon CloudWatch dashboards.
- B. Run the Amazon Kinesis Agent to write the status data to Amazon Kinesis Data Firehose Store the streaming data from Kinesis Data Firehose in Amazon Redshift
- C. (hen run a script on the pool data and analyze the data in Amazon Redshift
- D. Write the status data directly to a public Amazon S3 bucket from the health-checking component Configure S3 events to invoke an IAM Lambda function that analyzes the data
- E. Generate events from the health-checking component and send them to Amazon CloudWatch Events.Include the status data as event payload
- F. Use CloudWatch Events rules to invoke an IAM Lambda function that analyzes the data.

**Answer:** A

**Explanation:**

Amazon CloudWatch monitoring is a service that collects and tracks metrics from AWS resources and applications, and provides visualization tools and alarms to monitor performance and availability<sup>1</sup>. The health status data in JSON format can be sent to CloudWatch as custom metrics<sup>2</sup>, and then displayed in CloudWatch dashboards<sup>3</sup>. The other options are either inefficient or insecure for monitoring application availability in near-real time.

**NEW QUESTION 79**

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 principa
- 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 permission
- 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 permission
- H. Add the ARN of each service that needs the per-missions 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 actio
- K. Set the policy's resource field to the ARN of the service role.

**Answer:** BDF

**NEW QUESTION 81**

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 m the IAM Management Console and has installed me Amazon Inspector agent on an EC2 instances that need to be monitored.

Which additional steps should the Security Engineer lake 10 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 lo 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 86**

A security engineer wants to evaluate configuration changes to a specific AWS resource to ensure that the resource meets compliance standards. However, the security engineer is concerned about a situation in which several configuration changes are made to the resource in quick succession. The security engineer wants to record only the latest configuration of that resource to indicate the cumulative impact of the set of changes.

Which solution will meet this requirement in the MOST operationally efficient way?

- A. Use AWS CloudTrail to detect the configuration changes by filtering API calls to monitor the changes. Use the most recent API call to indicate the cumulative impact of multiple calls
- B. Use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes.
- C. Use Amazon CloudWatch to detect the configuration changes by filtering API calls to monitor the change
- D. Use the most recent API call to indicate the cumulative impact of multiple calls.
- E. Use AWS Cloud Map to detect the configuration change
- F. Generate a report of configuration changes from AWS Cloud Map to track the latest state by using a sliding time window.

**Answer:** B

**Explanation:**

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

To evaluate configuration changes to a specific AWS resource and ensure that it meets compliance standards, the security engineer should use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes. This will allow the security engineer to view the current state of the resource and its compliance status, as well as its configuration history and timeline.

AWS Config records configuration changes as ConfigurationItems, which are point-in-time snapshots of the resource's attributes, relationships, and metadata. If multiple configuration changes occur within a short period of time, AWS Config records only the latest ConfigurationItem for that resource. This indicates the cumulative impact of the set of changes on the resource's configuration.

This solution will meet the requirement in the most operationally efficient way, as it leverages AWS Config's features to monitor, record, and evaluate resource configurations without requiring additional tools or services.

The other options are incorrect because they either do not record the latest configuration in case of multiple configuration changes (A, C), or do not use a valid service for evaluating resource configurations (D).

Verified References:

- > <https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>
- > <https://docs.aws.amazon.com/config/latest/developerguide/config-item-table.html>

**NEW QUESTION 88**

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 91**

An organization must establish the ability to delete an IAM KMS Customer Master Key (CMK) within a 24- hour timeframe to keep it from being used for encrypt or decrypt operations Which of the following actions will address this requirement?

- A. Manually rotate a key within KMS to create a new CMK immediately
- B. Use the KMS import key functionality to execute a delete key operation
- C. Use the schedule key deletion function within KMS to specify the minimum wait period for deletion
- D. Change the KMS CMK alias to immediately prevent any services from using the CMK.

**Answer:** C

**Explanation:**

the schedule key deletion function within KMS allows you to specify a waiting period before deleting a customer master key (CMK)<sup>4</sup>. The minimum waiting period is 7 days and the maximum is 30 days<sup>5</sup>. This function prevents the CMK from being used for encryption or decryption operations during the waiting period<sup>4</sup>. The other options are either invalid or ineffective for deleting a CMK within a 24-hour timeframe.

**NEW QUESTION 94**

A company wants to configure DNS Security Extensions (DNSSEC) for the company's primary domain. The company registers the domain with Amazon Route 53. The company hosts the domain on Amazon EC2 instances by using BIND.

What is the MOST operationally efficient solution that meets this requirement?

- A. Set the dnssec-enable option to yes in the BIND configuratio
- B. Create a zone-signing key (ZSK) and a key-signing key (KSK) Restart the BIND service.
- C. Migrate the zone to Route 53 with DNSSEC signing enable
- D. Create a zone-signing key (ZSK) and a key-signing key (KSK) that are based on an AW



- E. Key Management Service (AWS KMS) customer managed key.
- F. Set the dnssec-enable option to yes in the BIND configuratio
- G. Create a zone-signing key (ZSK) and a key-signing key (KSK). Run the dnssec-signzone command to generate a delegation signer (DS) record Use AW
- H. Key Management Service (AWS KMS) to secure the keys.
- I. Migrate the zone to Route 53 with DNSSEC signing enable
- J. Create a key-signing key (KSK) that is based on an AWS Key Management Service (AWS KMS) customer managed ke
- K. Add a delegation signer (DS) record to the parent zone.

**Answer:** D

**Explanation:**

To configure DNSSEC for a domain registered with Route 53, the most operationally efficient solution is to migrate the zone to Route 53 with DNSSEC signing enabled, create a key-signing key (KSK) that is based on an AWS Key Management Service (AWS KMS) customer managed key, and add a delegation signer (DS) record to the parent zone. This way, Route 53 handles the zone-signing key (ZSK) and the signing of the records in the hosted zone, and the customer only needs to manage the KSK in AWS KMS and provide the DS record to the domain registrar. Option A is incorrect because it does not involve migrating the zone to Route 53, which would simplify the DNSSEC configuration. Option B is incorrect because it creates both a ZSK and a KSK based on AWS KMS customer managed keys, which is unnecessary and less efficient than letting Route 53 manage the ZSK. Option C is incorrect because it does not involve migrating the zone to Route 53, and it requires running the dnssec-signzone command manually, which is less efficient than letting Route 53 sign the zone automatically. Verified References:

- <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html>
- <https://aws.amazon.com/about-aws/whats-new/2020/12/announcing-amazon-route-53-support-dnssec/>

**NEW QUESTION 96**

A company is developing an ecommerce application. The application uses Amazon EC2 instances and an Amazon RDS MySQL database. For compliance reasons, data must be secured in transit and at rest. The company needs a solution that minimizes operational overhead and minimizes cost. Which solution meets these requirements?

- A. Use TLS certificates from AWS Certificate Manager (ACM) with an Application Load Balancer. Deploy self-signed certificates on the EC2 instance
- B. Ensure that the database client software uses a TLS connection to Amazon RD
- C. Enable encryption of the RDS DB instanc
- D. Enable encryption on the Amazon Elastic Block Store (Amazon EBS) volumes that support the EC2 instances.
- E. Use TLS certificates from a third-party vendor with an Application Load Balance
- F. Install the same certificates on the EC2 instance
- G. Ensure that the database client software uses a TLS connection to Amazon RD
- H. Use AWS Secrets Manager for client-side encryption of application data.
- I. Use AWS CloudHSM to generate TLS certificates for the EC2 instance
- J. Install the TLS certificates on the EC2 instance
- K. Ensure that the database client software uses a TLS connection to Amazon RD
- L. Use the encryption keys form CloudHSM for client-side encryption of application data.
- M. Use Amazon CloudFront with AWS WA
- N. Send HTTP connections to the origin EC2 instance
- O. Ensure that the database client software uses a TLS connection to Amazon RD
- P. Use AWS Key Management Service (AWS KMS) for client-side encryption of application data before the data is stored in the RDS database.

**Answer:** A

**NEW QUESTION 100**

A company is hosting multiple applications within a single VPC in its IAM account. The applications are running behind an Application Load Balancer that is associated with an IAM WAF web ACL. The company's security team has identified that multiple port scans are originating from a specific range of IP addresses on the internet.

A security engineer needs to deny access from the offending IP addresses. Which solution will meet these requirements?

- A. Modify the IAM WAF web ACL with an IP set match rule statement to deny incoming requests from the IP address range.
- B. Add a rule to all security groups to deny the incoming requests from the IP address range.
- C. Modify the IAM WAF web ACL with a rate-based rule statement to deny the incoming requests from the IP address range.
- D. Configure the IAM WAF web ACL with regex match condition
- E. Specify a pattern set to deny theincoming requests based on the match condition

**Answer:** A

**Explanation:**

Note that the IP is known and the question wants us to deny access from that particular address and so we can use IP set match policy of WAF to block access.

**NEW QUESTION 101**

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 105**

A developer signed in to a new account within an IAM Organization organizational unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP.

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

How can the security engineer provide the developer with Amazon S3 access without affecting other account?

- A. Move the SCP to the root OU of organization to remove the restriction to access Amazon S3.
- B. Add an IAM policy for the developer, which grants S3 access.
- C. Create a new OU without applying the SCP restricting S3 access.
- D. Move the developer account to this new OU.
- E. Add an allow list for the developer account for the S3 service.

**Answer: C**

**NEW QUESTION 110**

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 114**

A Development team has built an experimental environment to test a simple static 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 119**

A company is running internal microservices on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. The company is using Amazon Elastic Container Registry (Amazon ECR) private repositories.

A security engineer needs to encrypt the private repositories by using AWS Key Management Service (AWS KMS). The security engineer also needs to analyze the container images for any common vulnerabilities and exposures (CVEs).

Which solution will meet these requirements?

- A. Enable KMS encryption on the existing ECR repositories
- B. Install Amazon Inspector Agent from the ECS container instances' user data
- C. Run an assessment with the CVE rules.
- D. Recreate the ECR repositories with KMS encryption and ECR scanning enable
- E. Analyze the scan report after the next push of images.
- F. Recreate the ECR repositories with KMS encryption and ECR scanning enable
- G. Install AWS Systems Manager Agent on the ECS container instance
- H. Run an inventory report.
- I. Enable KMS encryption on the existing ECR repositories
- J. Use AWS Trusted Advisor to check the ECS container instances and to verify the findings against a list of current CVEs.

**Answer: B**

**NEW QUESTION 123**

A security engineer recently rotated the host keys for an Amazon EC2 instance. The security engineer is trying to access the EC2 instance by using the EC2 Instance Connect feature. However, the security engineer receives an error (or failed host key validation). Before the rotation of the host keys EC2 Instance Connect worked correctly with this EC2 instance.

What should the security engineer do to resolve this error?

- A. Import the key material into AWS Key Management Service (AWS KMS).
- B. Manually upload the new host key to the AWS trusted host keys database.
- C. Ensure that the AmazonSSMManagedInstanceCore policy is attached to the EC2 instance profile.
- D. Create a new SSH key pair for the EC2 instance.

**Answer: B**

**Explanation:**

To set up a CloudFront distribution for an S3 bucket that hosts a static website, and to allow only specified IP addresses to access the website, the following steps are required:

- Create a CloudFront origin access identity (OAI), which is a special CloudFront user that you can associate with your distribution. An OAI allows you to restrict access to your S3 content by using signed URLs or signed cookies. For more information, see [Using an origin access identity to restrict access to your Amazon S3 content](#).
- Create the S3 bucket policy so that only the OAI has access. This will prevent users from accessing the website directly by using S3 URLs, as they will receive an Access Denied error. To do this, use the AWS Policy Generator to create a bucket policy that grants s3:GetObject permission to the OAI, and attach it to the S3 bucket. For more information, see [Restricting access to Amazon S3 content by using an origin access identity](#).
- Create an AWS WAF web ACL and add an IP set rule. AWS WAF is a web application firewall service that lets you control access to your web applications. An IP set is a condition that specifies a list of IP addresses or IP address ranges that requests originate from. You can use an IP set rule to allow or block requests based on the IP addresses of the requesters. For more information, see [Working with IP match conditions](#).
- Associate the web ACL with the CloudFront distribution. This will ensure that the web ACL filters all requests for your website before they reach your origin. You can do this by using the AWS WAF console, API, or CLI. For more information, see [Associating or disassociating a web ACL with a CloudFront distribution](#). This solution will meet the requirements of allowing only specified IP addresses to access the website and preventing direct access by using S3 URLs. The other options are incorrect because they either do not create a CloudFront distribution for the S3 bucket (A), do not use an OAI to restrict access to the S3 bucket (C), or do not use AWS WAF to block traffic from outside the specified IP addresses (D).

Verified References:

- <https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-ip-conditions.html>

**NEW QUESTION 128**

A security engineer is configuring a new website that is named example.com. The security engineer wants to secure communications with the website by requiring users to connect to example.com through HTTPS.

Which of the following is a valid option for storing SSL/TLS certificates?

- A. Custom SSL certificate that is stored in AWS Key Management Service (AWS KMS)
- B. Default SSL certificate that is stored in Amazon CloudFront.
- C. Custom SSL certificate that is stored in AWS Certificate Manager (ACM)
- D. Default SSL certificate that is stored in Amazon S3

**Answer: C**

**NEW QUESTION 131**

A company's application team needs to host a MySQL database on IAM. According to the company's security policy, all data that is stored on IAM must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation.

The application team needs a solution that satisfies the company's security requirements and minimizes operational overhead.

Which solution will meet these requirements?

- A. Host the database on Amazon RD
- B. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an IAM Key Management Service (IAM KMS) custom key store that is backed by IAM CloudHSM for key management.
- C. Host the database on Amazon RD
- D. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an IAM managed CMK in IAM Key Management Service (IAM KMS) for key management.
- E. Host the database on an Amazon EC2 instance
- F. Use Amazon Elastic Block Store (Amazon EBS) for encryption
- G. Use a customer managed CMK in IAM Key Management Service (IAM KMS) for key management.
- H. Host the database on an Amazon EC2 instance
- I. Use Transparent Data Encryption (TDE) for encryption and key management.

**Answer:** B

#### NEW QUESTION 135

A security engineer is trying to use Amazon EC2 Image Builder to create an image of an EC2 instance. The security engineer has configured the pipeline to send logs to an Amazon S3 bucket. When the security engineer runs the pipeline, the build fails with the following error: "AccessDenied: Access Denied status code: 403".

The security engineer must resolve the error by implementing a solution that complies with best practices for least privilege access. Which combination of steps will meet these requirements? (Choose two.)

- A. Ensure that the following policies are attached to the IAM role that the security engineer is using: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.
- B. Ensure that the following policies are attached to the instance profile for the EC2 instance: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.
- C. Ensure that the AWSImageBuilderFullAccess policy is attached to the instance profile for the EC2 instance.
- D. Ensure that the security engineer's IAM role has the s3:PutObject permission for the S3 bucket.
- E. Ensure that the instance profile for the EC2 instance has the s3:PutObject permission for the S3 bucket.

**Answer:** BE

#### Explanation:

The most likely cause of the error is that the instance profile for the EC2 instance does not have the s3:PutObject permission for the S3 bucket. This permission is needed to upload logs to the bucket. Therefore, the security engineer should ensure that the instance profile has this permission.

One possible solution is to attach the AWSImageBuilderFullAccess policy to the instance profile for the EC2 instance. This policy grants full access to Image Builder resources and related AWS services, including the s3:PutObject permission for any bucket with "imagebuilder" in its name. However, this policy may grant more permissions than necessary, which violates the principle of least privilege.

Another possible solution is to create a custom policy that only grants the s3:PutObject permission for the specific S3 bucket that is used for logging. This policy can be attached to the instance profile along with the other policies that are required for Image Builder functionality: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore. This solution follows the principle of least privilege more closely than the previous one.

➤ Ensure that the following policies are attached to the instance profile for the EC2 instance: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.

➤ Ensure that the instance profile for the EC2 instance has the s3:PutObject permission for the S3 bucket.

This can be done by either attaching the AWSImageBuilderFullAccess policy or creating a custom policy with this permission.

1: Using managed policies for EC2 Image Builder - EC2 Image Builder 2: PutObject - Amazon Simple Storage Service 3: AWSImageBuilderFullAccess - AWS Managed Policy

#### NEW QUESTION 139

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

Please select:

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

**Answer:** A

#### Explanation:

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

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

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

Submit your Feedback/Queries to our Experts

#### NEW QUESTION 141

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

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



- F. Configure the application to connect to the NLB.
- G. Peer the on-premises network with the Kinesis Data Firehose VPC using Direct Connect.
- H. Configure the application to connect to the existing Firehose delivery stream.

**Answer:** A

**Explanation:**

To stream data using an existing Amazon Kinesis Data Firehose delivery stream and encrypt it in transit using a private network, the company should do the following:

- Create a VPC endpoint for Kinesis Data Firehose. This allows the company to use a private connection between their VPC and Kinesis Data Firehose without requiring an internet gateway or NAT device.
- Configure the application to connect to the VPC endpoint. This allows the application to stream data using Kinesis Data Firehose over AWS PrivateLink, which encrypts all traffic with TLS.

**NEW QUESTION 142**

A company has two VPCs in the same AWS Region and in the same AWS account. Each VPC uses a CIDR block that does not overlap with the CIDR block of the other VPC. One VPC contains AWS Lambda functions that run inside a subnet that accesses the internet through a NAT gateway. The Lambda functions require access to a publicly accessible Amazon Aurora MySQL database that is running in the other VPC.

A security engineer determines that the Aurora database uses a security group rule that allows connections from the NAT gateway IP address that the Lambda functions use. The company's security policy states that no database should be publicly accessible.

What is the MOST secure way that the security engineer can provide the Lambda functions with access to the Aurora database?

- A. Move the Aurora database into a private subnet that has no internet access routes in the database's current VPC. Configure the Lambda functions to use the Aurora database's new private IP address to access the database. Configure the Aurora database's security group to allow access from the private IP addresses of the Lambda functions.
- B. Establish a VPC endpoint between the two VPCs in the Aurora database's VPC. Configure a service VPC endpoint for Amazon RDS in the Lambda functions' VPC. Configure an interface VPC endpoint that uses the service endpoint in the Aurora database's VPC. Configure the service endpoint to allow connections from the Lambda functions.
- C. Establish an AWS Direct Connect interface between the VPCs. Configure the Lambda functions to use a new route table that accesses the Aurora database through the Direct Connect interface. Configure the Aurora database's security group to allow access from the Direct Connect interface IP address.
- D. Move the Lambda functions into a public subnet in their VPC. Move the Aurora database into a private subnet in its VPC. Configure the Lambda functions to use the Aurora database's new private IP address to access the database. Configure the Aurora database to allow access from the public IP addresses of the Lambda functions.

**Answer:** B

**Explanation:**

This option involves creating a VPC Endpoint between the two VPCs that allows private communication between them without going through the internet or exposing any public IP addresses. In this option, a VPC endpoint for Amazon RDS will be established, and an interface VPC endpoint will be created that points to the service endpoint in the Aurora database's VPC. This way, the Lambda functions can use the private IP address of the Aurora database to access it through the VPC endpoint without exposing any public IP addresses or allowing public internet access to the database.

**NEW QUESTION 147**

A company has two AWS accounts. One account is for development workloads. The other account is for production workloads. For compliance reasons, the production account contains all the AWS Key Management Service (AWS KMS) keys that the company uses for encryption.

The company applies an IAM role to an AWS Lambda function in the development account to allow secure access to AWS resources. The Lambda function must access a specific KMS customer managed key that exists in the production account to encrypt the Lambda function's data.

Which combination of steps should a security engineer take to meet these requirements? (Select TWO.)

- A. Configure the key policy for the customer managed key in the production account to allow access to the Lambda service.
- B. Configure the key policy for the customer managed key in the production account to allow access to the IAM role of the Lambda function in the development account.
- C. Configure a new IAM policy in the production account with permissions to use the customer managed key.
- D. Apply the IAM policy to the IAM role that the Lambda function in the development account uses.
- E. Configure a new key policy in the development account with permissions to use the customer managed key.
- F. Apply the key policy to the IAM role that the Lambda function in the development account uses.
- G. Configure the IAM role for the Lambda function in the development account by attaching an IAM policy that allows access to the customer managed key in the production account.

**Answer:** BE

**Explanation:**

To allow a Lambda function in one AWS account to access a KMS customer managed key in another AWS account, the following steps are required:

- Configure the key policy for the customer managed key in the production account to allow access to the IAM role of the Lambda function in the development account. A key policy is a resource-based policy that defines who can use or manage a KMS key. To grant cross-account access to a KMS key, you must specify the AWS account ID and the IAM role ARN of the external principal in the key policy statement. For more information, see [Allowing users in other accounts to use a KMS key](https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html).
- Configure the IAM role for the Lambda function in the development account by attaching an IAM policy that allows access to the customer managed key in the production account. An IAM policy is an identity-based policy that defines what actions an IAM entity can perform on which resources. To allow an IAM role to use a KMS key in another account, you must specify the KMS key ARN and the kms:Encrypt action (or any other action that requires access to the KMS key) in the IAM policy statement. For more information, see [Using IAM policies with AWS KMS](https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html).

This solution will meet the requirements of allowing secure access to a KMS customer managed key across AWS accounts.

The other options are incorrect because they either do not grant cross-account access to the KMS key (A, C), or do not use a valid policy type for KMS keys (D).

Verified References:

- <https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html>

**NEW QUESTION 152**

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



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

Which steps would help achieve this? (Select TWO.)

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

**Answer:** BE

**Explanation:**

To minimize downtime in response to DDoS attacks, the company should do the following:

- Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack. This provides access to 24x7 support from the AWS DDoS Response Team (DRT), as well as advanced detection and mitigation capabilities for network and application layer attacks.
- Use AWS WAF to create rules to respond to such attacks. This allows the company to filter web requests based on IP addresses, headers, body, or URI strings, and block malicious requests before they reach the web applications.

**NEW QUESTION 156**

A company has an AWS Lambda function that creates image thumbnails from larger images. The Lambda function needs read and write access to an Amazon S3 bucket in the same AWS account.

Which solutions will provide the Lambda function this access? (Select TWO.)

- A. Create an IAM user that has only programmatic access.
- B. Create a new access key pair.
- C. Add environmental variables to the Lambda function with the access key ID and secret access key.
- D. Modify the Lambda function to use the environmental variables at run time during communication with Amazon S3.
- E. Generate an Amazon EC2 key pair.
- F. Store the private key in AWS Secrets Manager.
- G. Modify the Lambda function to retrieve the private key from Secrets Manager and to use the private key during communication with Amazon S3.
- H. Create an IAM role for the Lambda function.
- I. Attach an IAM policy that allows access to the S3 bucket.
- J. Create an IAM role for the Lambda function.
- K. Attach a bucket policy to the S3 bucket to allow access. Specify the function's IAM role as the principal.
- L. Create a security group.
- M. Attach the security group to the Lambda function.
- N. Attach a bucket policy that allows access to the S3 bucket through the security group ID.

**Answer:** CD

**NEW QUESTION 158**

A company is hosting a static website on Amazon S3. The company has configured an Amazon CloudFront distribution to serve the website contents. The company has associated an IAM WAF web ACL with the CloudFront distribution. The web ACL ensures that requests originate from the United States to address compliance restrictions.

The company is worried that the S3 URL might still be accessible directly and that requests can bypass the CloudFront distribution.

Which combination of steps should the company take to remove direct access to the S3 URL? (Select TWO.)

- A. Select "Restrict Bucket Access" in the origin settings of the CloudFront distribution.
- B. Create an origin access identity (OAI) for the S3 origin.
- C. Update the S3 bucket policy to allow s3:GetObject with a condition that the IAM:Referer key matches the secret value. Deny all other requests.
- D. Configure the S3 bucket policy so that only the origin access identity (OAI) has read permission for objects in the bucket.
- E. Add an origin custom header that has the name Referer to the CloudFront distribution. Give the header a secret value.

**Answer:** AD

**NEW QUESTION 159**

A company has a large fleet of Linux Amazon EC2 instances and Windows EC2 instances that run in private subnets. The company wants all remote administration to be performed as securely as possible in the AWS Cloud.

Which solution will meet these requirements?

- A. Do not use SSH-RSA private keys during the launch of new instance.
- B. Implement AWS Systems Manager Session Manager.
- C. Generate new SSH-RSA private keys for existing instance.
- D. Implement AWS Systems Manager Session Manager.
- E. Do not use SSH-RSA private keys during the launch of new instance.
- F. Configure EC2 Instance Connect.
- G. Generate new SSH-RSA private keys for existing instance.
- H. Configure EC2 Instance Connect.

**Answer:** A

**Explanation:**

AWS Systems Manager Session Manager is a fully managed service that allows you to securely and remotely administer your EC2 instances without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager provides an interactive browser-based shell or CLI access to your instances, as well as port forwarding and auditing capabilities. Session Manager works with both Linux and Windows instances, and supports hybrid environments and edge devices.

EC2 Instance Connect is a feature that allows you to use SSH to connect to your Linux instances using

short-lived keys that are generated on demand and delivered securely through the AWS metadata service. EC2 Instance Connect does not require any additional software installation or configuration on the instance, but it does require you to use SSH-RSA keys during the launch of new instances.

The correct answer is to use Session Manager, as it provides more security and flexibility than EC2 Instance Connect, and does not require SSH-RSA keys or inbound ports. Session Manager also works with Windows instances, while EC2 Instance Connect does not.

Verified References:

- <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>
- <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html>
- <https://repost.aws/questions/QUnV4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec-2-ins>

#### NEW QUESTION 161

A company wants to migrate its static primary domain website to AWS. The company hosts the website and DNS servers internally. The company wants the website to enforce SSL/TLS encryption block IP addresses from outside the United States (US), and take advantage of managed services whenever possible. Which solution will meet these requirements?

- A. Migrate the website to Amazon S3 Import a public SSL certificate to an Application Load Balancer
- B. Balancer with rules to block traffic from outside the US Migrate DNS to Amazon Route 53.
- C. Migrate the website to Amazon EC2 Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to an Application Load Balancer with rules to block traffic from outside the US Update DNS accordingly.
- D. Migrate the website to Amazon S3. Import a public SSL certificate to Amazon CloudFront Use AWS WAF rules to block traffic from outside the US Update DNS accordingly
- E. Migrate the website to Amazon S3 Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to Amazon CloudFront
- F. CloudFront Configure CloudFront to block traffic from outside the US
- G. Migrate DNS to Amazon Route 53.

**Answer: D**

#### Explanation:

To migrate the static website to AWS and meet the requirements, the following steps are required:

- Migrate the website to Amazon S3, which is a highly scalable and durable object storage service that can host static websites. To do this, create an S3 bucket with the same name as the domain name of the website, enable static website hosting for the bucket, upload the website files to the bucket, and configure the bucket policy to allow public read access to the objects. For more information, see [Hosting a static website on Amazon S3](#).
  - Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to Amazon CloudFront, which is a global content delivery network (CDN) service that can improve the performance and security of web applications. To do this, request or import a public SSL certificate for the domain name of the website using ACM, create a CloudFront distribution with the S3 bucket as the origin, and associate the SSL certificate with the distribution. For more information, see [Using alternate domain names and HTTPS](#).
  - Configure CloudFront to block traffic from outside the US, which is one of the requirements. To do this, create a CloudFront web ACL using AWS WAF, which is a web application firewall service that lets you control access to your web applications. In the web ACL, create a rule that uses a geo match condition to block requests that originate from countries other than the US. Associate the web ACL with the CloudFront distribution. For more information, see [How AWS WAF works with Amazon CloudFront features](#).
  - Migrate DNS to Amazon Route 53, which is a highly available and scalable cloud DNS service that can route traffic to various AWS services. To do this, register or transfer your domain name to Route 53, create a hosted zone for your domain name, and create an alias record that points your domain name to your CloudFront distribution. For more information, see [Routing traffic to an Amazon CloudFront web distribution by using your domain name](#).
- The other options are incorrect because they either do not implement SSL/TLS encryption for the website (A), do not use managed services whenever possible (B), or do not block IP addresses from outside the US (C). Verified References:

- <https://docs.aws.amazon.com/AmazonS3/latest/userguide/HostingWebsiteOnS3Setup.html>
- <https://docs.aws.amazon.com/waf/latest/developerguide/waf-cloudfront.html>
- <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html>

#### NEW QUESTION 163

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

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

**Answer: C**

#### Explanation:

The correct answer is C. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.

According to the AWS documentation<sup>1</sup>, a bucket policy is a resource-based policy that you can use to grant access permissions to your Amazon S3 bucket and the objects in it. Only the bucket owner can associate a policy with a bucket. The permissions attached to the bucket apply to all of the objects in the bucket that are owned by the bucket owner.

When you create a trail in CloudTrail, you can specify an existing S3 bucket or create a new one to store your log files. CloudTrail automatically creates a bucket policy for your S3 bucket that grants CloudTrail write-only access to deliver log files to your bucket. The bucket policy also grants read-only access to AWS services that you can use to view and analyze your log data, such as Amazon Athena, Amazon CloudWatch Logs, and Amazon QuickSight.

If you want to update the log file prefix for an existing trail, you must also update the existing bucket policy in the S3 console with the new log file prefix. The log file prefix is part of the resource ARN that identifies the objects in your bucket that CloudTrail can access. If you don't update the bucket policy with the new log file prefix, CloudTrail will not be able to deliver log files to your bucket, and you will receive an error message when you try to save the change in the CloudTrail console.

The other options are incorrect because:

- A. Creating a new trail with the updated log file prefix, and then deleting the original trail is not necessary and may cause data loss or inconsistency. You can

simply update the existing trail and its associated bucket policy with the new log file prefix.

➤ B. Updating the existing bucket policy in the S3 console to allow the Security Engineer's Principal to perform PutBucketPolicy is not relevant to this issue. The PutBucketPolicy action allows you to create or replace a policy on a bucket, but it does not affect CloudTrail's ability to deliver log files to your bucket. You still need to update the existing bucket policy with the new log file prefix.

➤ D. Updating the existing bucket policy in the S3 console to allow the Security Engineer's Principal to perform GetBucketPolicy is not relevant to this issue. The GetBucketPolicy action allows you to retrieve a policy on a bucket, but it does not affect CloudTrail's ability to deliver log files to your bucket. You still need to update the existing bucket policy with the new log file prefix.

References:

1: Using bucket policies - Amazon Simple Storage Service

#### NEW QUESTION 167

A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.

All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.

Which SCP should the security engineer attach to the root of the organization to meet these requirements? A)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "guardduty:DeleteDetector",
        "guardduty:UpdateDetector",
        "securityhub:DisableSecurityHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

B)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "NotAction": [
        "guardduty:DeleteDetector",
        "guardduty:UpdateDetector",
        "securityhub:DisableSecurityHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

C)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "guardduty:DeleteDetector",
        "guardduty:UpdateDetector",
        "securityhub:DisableSecurityHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

D)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "NotAction": [
        "guardduty:DeleteDetector",
        "guardduty:UpdateDetector",
        "securityhub:DisableSecurityHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

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

**Answer: A**

#### NEW QUESTION 171

A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.

A security engineer must automate a response in the company's organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company's security team.

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

- A. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role.
- B. Configure the state machine to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role.
- D. Configure the AWS Batch job to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
- E. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.
- F. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.
- G. Create an Amazon Simple Queue Service (Amazon SQS) queue.
- H. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.
- I. Create an Amazon Simple Notification Service (Amazon SNS) topic for external or cross-account access notice.
- J. Subscribe the security team's email addresses to the topic.

**Answer: ACF**

#### Explanation:

The correct answer is A, C, and F.

To automate a response for any newly created policies that are overly permissive, the security engineer needs to use a combination of services that can monitor, analyze, remediate, and notify the security incidents.

Option A is correct because creating an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role is a valid way to remediate external access. AWS Step Functions is a service that allows you to coordinate multiple AWS services into serverless workflows. You can use Step Functions to invoke AWS Lambda functions, which can modify the IAM policies programmatically. You can also use Step



Functions to publish a notification to an Amazon SNS topic, which can send messages to subscribers such as email addresses.

Option B is incorrect because creating an AWS Batch job that forwards any resource type findings to an AWS Lambda function is not a suitable way to automate a response. AWS Batch is a service that enables you to run batch computing workloads on AWS. Batch is designed for large-scale and long-running jobs that can benefit from parallelization and dynamic provisioning of compute resources. Batch is not intended for event-driven and real-time workflows that require immediate response.

Option C is correct because creating an Amazon EventBridge event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution is a valid way to monitor and analyze the security incidents. Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from various sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke AWS Step Functions state machines from the IAM Access Analyzer findings.

Option D is incorrect because creating an Amazon CloudWatch metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution is not a suitable way to monitor and analyze the security incidents. Amazon CloudWatch is a service that provides monitoring and observability for your AWS resources and applications. CloudWatch can collect metrics, logs, and events from various sources and perform actions based on alarms or filters. However, CloudWatch cannot directly invoke AWS Batch jobs from the IAM Access Analyzer findings. You would need to use another service such as EventBridge or SNS to trigger the Batch job.

Option E is incorrect because creating an Amazon SQS queue that forwards a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked is not a valid way to notify the security incidents. Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS can deliver messages to consumers that poll the queue for messages. However, SQS cannot directly forward a notification to the security team's email addresses. You would need to use another service such as SNS or SES to send email notifications.

Option F is correct because creating an Amazon SNS topic for external or cross-account access notices and subscribing the security team's email addresses to the topic is a valid way to notify the security incidents. 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 use SNS to send email notifications to the security team when a critical security finding is detected.

References:

- AWS Step Functions
- AWS Batch
- Amazon EventBridge
- Amazon CloudWatch
- Amazon SQS
- Amazon SNS

## NEW QUESTION 173

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questons 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](#)**