

# Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

<https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/>



#### NEW QUESTION 1

A company uses Amazon Elastic Container Service (Amazon ECS) containers that have the Fargate launch type. The containers run web and mobile applications that are written in Java and Node.js. To meet network segmentation requirements, each of the company's business units deploys applications in its own dedicated AWS account.

Each business unit stores container images in an Amazon Elastic Container Registry (Amazon ECR) private registry in its own account.

A security engineer must recommend a solution to scan ECS containers and ECR registries for vulnerabilities in operating systems and programming language libraries.

The company's audit team must be able to identify potential vulnerabilities that exist in any of the accounts where applications are deployed.

Which solution will meet these requirements?

- A. In each account, update the ECR registry to use Amazon Inspector instead of the default scanning service
- B. Configure Amazon Inspector to forward vulnerability findings to AWS Security Hub in a central security account
- C. Provide access for the audit team to use Security Hub to review the findings.
- D. In each account, configure AWS Config to monitor the configuration of the ECS containers and the ECR registry
- E. Configure AWS Config conformance packs for vulnerability scanning
- F. Create an AWS Config aggregator in a central account to collect configuration and compliance details from all accounts
- G. Provide the audit team with access to AWS Config in the account where the aggregator is configured.
- H. In each account, configure AWS Audit Manager to scan the ECS containers and the ECR registry. Configure Audit Manager to forward vulnerability findings to AWS Security Hub in a central security account
- I. Provide access for the audit team to use Security Hub to review the findings.
- J. In each account, configure Amazon GuardDuty to scan the ECS containers and the ECR registry. Configure GuardDuty to forward vulnerability findings to AWS Security Hub in a central security account
- K. Provide access for the audit team to use Security Hub to review the findings.

**Answer: B**

#### Explanation:

➤ Option B: This option meets the requirements of scanning ECS containers and ECR registries for vulnerabilities, and providing a centralized view of the findings for the audit team. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config conformance packs are a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations. Conformance packs can help you manage configuration compliance of your AWS resources at scale by using a common framework and packaging model. You can use prebuilt conformance packs for vulnerability scanning, such as CIS Operating System Security Configuration Benchmarks or Amazon Inspector Rules for Linux Instances<sup>1</sup>. You can also create custom conformance packs to scan for vulnerabilities in programming language libraries. AWS Config aggregator is a feature that enables you to aggregate configuration and compliance data from multiple accounts and Regions into a single account and Region<sup>2</sup>. You can provide access for the audit team to use AWS Config in the account where the aggregator is configured, and view the aggregated data in the AWS Config console or API.

#### NEW QUESTION 2

A company deployed IAM Organizations to help manage its increasing number of IAM accounts. A security engineer wants to ensure only principals in the Organization structure can access a specific Amazon S3 bucket. The solution must also minimize operational overhead

Which solution will meet these requirements?

- A. 1 Put all users into an IAM group with an access policy granting access to the S3 bucket.
- B. Have the account creation trigger an IAM Lambda function that manages the bucket policy, allowing access to accounts listed in the policy only.
- C. Add an SCP to the Organizations master account, allowing all principals access to the bucket.
- D. Specify the organization ID in the global key condition element of a bucket policy, allowing all principals access.

**Answer: D**

#### NEW QUESTION 3

A company discovers a billing anomaly in its AWS account. A security consultant investigates the anomaly and discovers that an employee who left the company 30 days ago still has access to the account.

The company has not monitored account activity in the past.

The security consultant needs to determine which resources have been deployed or reconfigured by the employee as quickly as possible.

Which solution will meet these requirements?

- A. In AWS Cost Explorer, filter chart data to display results from the past 30 days
- B. Export the results to a data table
- C. Group the data table by resource
- D. Use AWS Cost Anomaly Detection to create a cost monitor
- E. Access the detection history
- F. Set the time frame to Last 30 days
- G. In the search area, choose the service category.
- H. In AWS CloudTrail, filter the event history to display results from the past 30 days
- I. Create an Amazon Athena table that contains the data
- J. Partition the table by event source.
- K. Use AWS Audit Manager to create an assessment for the past 30 days
- L. Apply a usage-based framework to the assessments
- M. Configure the assessment to assess by resource.

**Answer: C**

#### NEW QUESTION 4

A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region. The DB cluster is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. To meet compliance requirements, the company needs to copy a DB snapshot to the us-west-1 Region. However, when the company tries to copy the snapshot to us-west-1 the company cannot access the key that was used to encrypt the original database.

What should the company do to set up the snapshot in us-west-1 with proper encryption?

- A. Use AWS Secrets Manager to store the customer managed key in us-west-1 as a secret Use this secret to encrypt the snapshot in us-west-1.
- B. Create a new customer managed key in us-west-1. Use this new key to encrypt the snapshot in us-west-1.
- C. Create an IAM policy that allows access to the customer managed key in us-east-1. Specify am aws kmsus-west-1 " as the principal.
- D. Create an IAM policy that allows access to the customer managed key in us-east-1. Specify arn aws rds us-west-1. \* as the principal.

**Answer: B**

**Explanation:**

"If you copy an encrypted snapshot across Regions, you must specify a KMS key valid in the destination AWS Region. It can be a Region-specific KMS key, or a multi-Region key." <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-copy-snapshot.html#aurora-copy-sna>

**NEW QUESTION 5**

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 6**

A recent security audit found that IAM CloudTrail logs are insufficiently protected from tampering and unauthorized access Which actions must the Security Engineer take to address these audit findings? (Select THREE )

- A. Ensure CloudTrail log file validation is turned on
- B. Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long-term storage
- C. Use an S3 bucket with tight access controls that exists in a separate account
- D. Use Amazon Inspector to monitor the file integrity of CloudTrail log files.
- E. Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files
- F. Encrypt the CloudTrail log files with server-side encryption with IAM KMS-managed keys (SSE-KMS)

**Answer: ADE**

**NEW QUESTION 7**

A company's engineering team is developing a new application that creates IAM Key Management Service (IAM KMS) CMK grants for users immediately after a grant is created users must be able to use the CMK to encrypt a 512-byte payload. During load testing, a bug appears intermittently where AccessDeniedExceptions are occasionally triggered when a user first attempts to encrypt using the CMK Which solution should the company's security specialist recommend?

- A. Instruct users to implement a retry mechanism every 2 minutes until the call succeeds.
- B. Instruct the engineering team to consume a random grant token from users, and to call the CreateGrant operation, passing it the grant token
- C. Instruct users to use that grant token in their call to encrypt.
- D. Instruct the engineering team to create a random name for the grant when calling the CreateGrant operation
- E. Return the name to the users and instruct them to provide the name as the grant token in the call to encrypt.
- F. Instruct the engineering team to pass the grant token returned in the CreateGrant response to users. Instruct users to use that grant token in their call to encrypt.

**Answer:** D

**Explanation:**

To avoid AccessDeniedExceptions when users first attempt to encrypt using the CMK, the security specialist should recommend the following solution:

- Instruct the engineering team to pass the grant token returned in the CreateGrant response to users. This allows the engineering team to use the grant token as a form of temporary authorization for the grant.
- Instruct users to use that grant token in their call to encrypt. This allows the users to use the grant token as a proof that they have permission to use the CMK, and to avoid any eventual consistency issues with the grant creation.

**NEW QUESTION 8**

Auditors for a health care company have mandated that all data volumes be encrypted at rest Infrastructure is deployed mainly via IAM CloudFormation however third-party frameworks and manual deployment are required on some legacy systems  
 What is the BEST way to monitor, on a recurring basis, whether all EBS volumes are encrypted?

- A. On a recurring basis, update an IAM user policies to require that EC2 instances are created with an encrypted volume
- B. Configure an IAM Config rule to run on a recurring basis for volume encryption
- C. Set up Amazon Inspector rules for volume encryption to run on a recurring schedule
- D. Use CloudWatch Logs to determine whether instances were created with an encrypted volume

**Answer:** B

**Explanation:**

To support answer B, use the reference <https://d1.IAMstatic.com/whitepapers/IAM-security-whitepaper.pdf> "For example, IAM Config provides a managed IAM Config Rules to ensure that encryption is turned on for all EBS volumes in your account."

**NEW QUESTION 9**

A System Administrator is unable to start an Amazon EC2 instance in the eu-west-1 Region using an IAM role The same System Administrator is able to start an EC2 instance in the eu-west-2 and eu-west-3 Regions. The IAMSystemAdministrator access policy attached to the System Administrator IAM role allows unconditional access to all IAM services and resources within the account  
 Which configuration caused this issue?

A) An SCP is attached to the account with the following permission statement:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "All",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "iam:*",
        "organizations:*",
        "route53:*",
        "budgets:*",
        "waf:*",
        "cloudfront:*",
        "globalaccelerator:*",
        "importexport:*",
        "support:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": [
            "eu-west-*"
          ]
        }
      }
    }
  ]
}
```

- B)
- A permission boundary policy is attached to the System Administrator role with the following permission statement:



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "iam:*",
        "organizations:*",
        "route53:*",
        "budgets:*",
        "waf:*",
        "cloudfront:*",
        "globalaccelerator:*",
        "importexport:*",
        "support:*",
        "ec2:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        }
      }
    }
  ]
}
```

C)  
 A permission boundary is attached to the System Administrator role with the following permission statement:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*"
      ],
      "Resource": "*"
    },
    {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Action": "ec2:*",
          "Resource": "*",
          "Condition": {
            "StringEquals": {
              "aws:RequestedRegion": [
                "eu-west-1"
              ]
            }
          }
        }
      ]
    }
  ]
}
```

D)  
 An SCP is attached to the account with the following statement:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "iam:*",
        "organizations:*",
        "route53:*",
        "budgets:*",
        "waf:*",
        "cloudfront:*",
        "globalaccelerators:*",
        "importexport:*",
        "support:*",
        "ec2:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}

```

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

**Answer: B**

#### NEW QUESTION 10

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 10

A developer has created an AWS Lambda function in a company's development account. The Lambda function requires the use of an AWS Key Management Service (AWS KMS) customer managed key that exists in a security account that the company's security team controls. The developer obtains the ARN of the KMS key from a previous Lambda function in the development account. The previous Lambda function had been working properly with the KMS key. When the developer uses the ARN and tests the new Lambda function an error message states that access is denied to the KMS key in the security account. The developer tests the previous Lambda function that uses the same KMS key and discovers that the previous Lambda function still can encrypt data as expected. A security engineer must resolve the problem so that the new Lambda function in the development account can use the KMS key from the security account. Which combination of steps should the security engineer take to meet these requirements? (Select TWO.)

- A. In the security account configure an IAM role for the new Lambda function
- B. Attach an IAM policy that allows access to the KMS key in the security account.
- C. In the development account configure an IAM role for the new Lambda function
- D. Attach a key policy that allows access to the KMS key in the security account.
- E. In the development account configure an IAM role for the new Lambda function
- F. Attach an IAM policy that allows access to the KMS key in the security account.
- G. Configure a key policy for the KMS key in the security account to allow access to the IAM role of the new Lambda function in the security account.
- H. Configure a key policy for the KMS key in the security account to allow access to the IAM role of the new Lambda function in the development account.

**Answer: CE**

#### Explanation:

To allow cross-account access to a KMS key, the key policy of the KMS key must grant permission to the external account or principal, and the IAM policy of the external account or principal must delegate the key policy permission. In this case, the new Lambda function in the development account needs to use the KMS key in the security account, so the key policy of the KMS key must allow access to the IAM role of the new Lambda function in the development account (option E), and the IAM role of the new Lambda function in the development account must have an IAM policy that allows access to the KMS key in the security account (option C). Option A is incorrect because it creates an IAM role for the new Lambda function in the security account, not in the development account. Option B is incorrect because it attaches a key policy to an IAM role, which is not valid. Option D is incorrect because it allows access to the IAM role of the new Lambda function in the security account, not in the development account. Verified References:

➤ <https://docs.aws.amazon.com/autoscaling/ec2/userguide/key-policy-requirements-EBS-encryption.html>

### NEW QUESTION 13

A company finds that one of its Amazon EC2 instances suddenly has a high CPU usage. The company does not know whether the EC2 instance is compromised or whether the operating system is performing background cleanup.

Which combination of steps should a security engineer take before investigating the issue? (Select THREE.)

- A. Disable termination protection for the EC2 instance if termination protection has not been disabled.
- B. Enable termination protection for the EC2 instance if termination protection has not been enabled.
- C. Take snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.
- D. Remove all snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.
- E. Capture the EC2 instance metadata, and then tag the EC2 instance as under quarantine.
- F. Immediately remove any entries in the EC2 instance metadata that contain sensitive information.

**Answer:** BCE

#### Explanation:

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

### NEW QUESTION 15

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

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

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

**Answer:** AD

### NEW QUESTION 20

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](#).

➤ 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](#).

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 25

A company's cloud operations team is responsible for building effective security for IAM cross-account access. The team asks a security engineer to help

troubleshoot why some developers in the developer account (123456789012) in the developers group are not able to assume a cross-account role (ReadS3) into a production account (999999999999) to read the contents of an Amazon S3 bucket (productionapp). The two account policies are as follows:

Developer account 123456789012:

Developer group permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::999999999999:role/ReadS3"
    }
  ]
}
```

Production account 999999999999:

Production account ReadS3 role policy:

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

Production account ReadS3 role policy - trust relationship:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::888888888888:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "BoolIfExists": {
          "aws:MultiFactorAuthPresent": "true"
        }
      }
    }
  ]
}
```

Which recommendations should the security engineer make to resolve this issue? (Select TWO.)

- A. Ask the developers to change their password and use a different web browser.
- B. Ensure that developers are using multi-factor authentication (MFA) when they log in to their developer account as the developer role.
- C. Modify the production account ReadS3 role policy to allow the PutBucketPolicy action on the productionapp S3 bucket.
- D. Update the trust relationship policy on the production account S3 role to allow the account number of the developer account.
- E. Update the developer group permissions in the developer account to allow access to the productionapp S3 bucket.

Answer: AD

#### NEW QUESTION 29

While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139).

The ping command did not return a response. The flow log in the VPC showed the following:

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

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

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



D. In the VPC's NACL, allow outbound ICMP traffic.

**Answer:** D

### NEW QUESTION 33

A company stores images for a website in an Amazon S3 bucket. The company is using Amazon CloudFront to serve the images to end users. The company recently discovered that the images are being accessed from countries where the company does not have a distribution license. Which actions should the company take to secure the images to limit 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:

To secure the images to limit their distribution, the company should take the following actions:

- Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI). This allows the company to use a special CloudFront user that can access objects in their S3 bucket, and prevent anyone else from accessing them directly.
- Add a CloudFront geo restriction deny list of countries where the company lacks a license. This allows the company to use a feature that controls access to their content based on the geographic location of their viewers, and block requests from countries where they do not have a distribution license.

### NEW QUESTION 37

A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.

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

- A. Pull images from the public container registr
- B. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account
- C. Use a CI/CD pipeline to deploy the images to different AWS account
- D. Use identity-based policies to restrict access to which IAM principals can access the images.
- E. Pull images from the public container registr
- F. Publish the images to a private container registry that is hosted on Amazon EC2 instances in a centralized AWS account
- G. Deploy host-based container scanning tools to EC2 instances that run Amazon EC
- H. Restrict access to the container images by using basic authentication over HTTPS.
- I. Pull images from the public container registr
- J. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account
- K. Use a CI/CD pipeline to deploy the images to different AWS account
- L. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
- M. Pull images from the public container registr
- N. Publish the images to AWS CodeArtifact repositories in a centralized AWS account
- O. Use a CI/CD pipeline to deploy the images to different AWS account
- P. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

**Answer:** C

#### Explanation:

The correct answer is C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account.

Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

This solution meets the requirements because:

- Amazon ECR is a fully managed container registry service that supports Docker and OCI images and artifacts<sup>1</sup>. It integrates with Amazon ECS and other AWS services to simplify the development and deployment of container-based applications.
- Amazon ECR provides image scanning on push, which uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project to detect software vulnerabilities in container images<sup>2</sup>. The scan results are available in the AWS Management Console, AWS CLI, or AWS SDKs<sup>2</sup>.
- Amazon ECR supports cross-account access to repositories, which allows sharing images across multiple AWS accounts<sup>3</sup>. This can be achieved by using repository policies, which are resource-based policies that specify which IAM principals and accounts can access the repositories and what actions they can perform<sup>4</sup>. Additionally, identity-based policies can be used to control which IAM roles in each account can access the repositories<sup>5</sup>.

The other options are incorrect because:

- A. This option does not use repository policies to restrict cross-account access to the images, which is a requirement. Identity-based policies alone are not sufficient to control access to Amazon ECR repositories<sup>5</sup>.
- B. This option does not use Amazon ECR, which is a fully managed service that provides image scanning and cross-account access features. Hosting a private container registry on EC2 instances would require more management overhead and additional security measures.
- D. This option uses AWS CodeArtifact, which is a fully managed artifact repository service that supports Maven, npm, NuGet, PyPI, and generic package formats<sup>6</sup>. However, AWS CodeArtifact does not support Docker or OCI container images, which are required for Amazon ECS applications.

### NEW QUESTION 38

A company has an application that uses dozens of Amazon DynamoDB tables to store data. Auditors find that the tables do not comply with the company's data protection policy.

The company's retention policy states that all data must be backed up twice each month: once at midnight on the 15th day of the month and again at midnight on the 25th day of the month. The company must retain the backups for 3 months.

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

- A. Use the DynamoDB on-demand backup capability to create a backup plan.
- B. Configure a lifecycle policy to expire backups after 3 months.
- C. Use AWS DataSync to create a backup plan.
- D. Add a backup rule that includes a retention period of 3 months.
- E. Use AWS Backup to create a backup plan.
- F. Add a backup rule that includes a retention period of 3 months.
- G. Set the backup frequency by using a cron schedule expression.
- H. Assign each DynamoDB table to the backup plan.
- I. Set the backup frequency by using a rate schedule expression.
- J. Assign each DynamoDB table to the backup plan.

**Answer:** AD

#### NEW QUESTION 41

A company has two teams, and each team needs to access its respective Amazon S3 buckets. The company anticipates adding more teams that also will have their own S3 buckets. When the company adds these teams, team members will need the ability to be assigned to multiple teams. Team members also will need the ability to change teams. Additional S3 buckets can be created or deleted.

An IAM administrator must design a solution to accomplish these goals. The solution also must be scalable and must require the least possible operational overhead.

Which solution meets these requirements?

- A. Add users to groups that represent the team.
- B. Create a policy for each team that allows the team to access its respective S3 buckets only.
- C. Attach the policy to the corresponding group.
- D. Create an IAM role for each team.
- E. Create a policy for each team that allows the team to access its respective S3 buckets only.
- F. Attach the policy to the corresponding role.
- G. Create IAM roles that are labeled with an access tag value of a team.
- H. Create one policy that allows dynamic access to S3 buckets with the same tag.
- I. Attach the policy to the IAM role.
- J. Tag the S3 buckets accordingly.
- K. Implement a role-based access control (RBAC) authorization mode.
- L. Create the corresponding policies, and attach them to the IAM users.

**Answer:** A

#### NEW QUESTION 43

An AWS account that is used for development projects has a VPC that contains two subnets. The first subnet is named public-subnet-1 and has the CIDR block 192.168.1.0/24 assigned. The other subnet is named private-subnet-2 and has the CIDR block 192.168.2.0/24 assigned. Each subnet contains Amazon EC2 instances.

Each subnet is currently using the VPC's default network ACL. The security groups that the EC2 instances in these subnets use have rules that allow traffic between each instance where required. Currently, all network traffic flow is working as expected between the EC2 instances that are using these subnets.

A security engineer creates a new network ACL that is named subnet-2-NACL with default entries. The security engineer immediately configures private-subnet-2 to use the new network ACL and makes no other changes to the infrastructure. The security engineer starts to receive reports that the EC2 instances in public-subnet-1 and public-subnet-2 cannot communicate with each other.

Which combination of steps should the security engineer take to allow the EC2 instances that are running in these two subnets to communicate again? (Select TWO.)

- A. Add an outbound allow rule for 192.168.2.0/24 in the VPC's default network ACL.
- B. Add an inbound allow rule for 192.168.2.0/24 in the VPC's default network ACL.
- C. Add an outbound allow rule for 192.168.2.0/24 in subnet-2-NACL.
- D. Add an inbound allow rule for 192.168.1.0/24 in subnet-2-NACL.
- E. Add an outbound allow rule for 192.168.1.0/24 in subnet-2-NACL.

**Answer:** CE

#### Explanation:

The AWS documentation states that you can add an outbound allow rule for 192.168.2.0/24 in

subnet-2-NACL and add an outbound allow rule for 192.168.1.0/24 in subnet-2-NACL. This will allow the EC2 instances that are running in these two subnets to communicate again.

References: : Amazon VPC User Guide

#### NEW QUESTION 47

A company in France uses Amazon Cognito with the Cognito Hosted UI as an identity broker for sign-in and sign-up processes. The company is marketing an application and expects that all the application's users will come from France.

When the company launches the application the company's security team observes fraudulent sign-ups for the application. Most of the fraudulent registrations are from users outside of France.

The security team needs a solution to perform custom validation at sign-up. Based on the results of the validation the solution must accept or deny the registration request.

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 50**

A security engineer needs to develop a process to investigate and respond to potential security events on a company's Amazon EC2 instances. All the EC2 instances are backed by Amazon Elastic Block Store (Amazon EBS). The company uses AWS Systems Manager to manage all the EC2 instances and has installed Systems Manager Agent (SSM Agent) on all the EC2 instances.

The process that the security engineer is developing must comply with AWS security best practices and must meet the following requirements:

- A compromised EC2 instance's volatile memory and non-volatile memory must be preserved for forensic purposes.
- A compromised EC2 instance's metadata must be updated with corresponding incident ticket information.
- A compromised EC2 instance must remain online during the investigation but must be isolated to prevent the spread of malware.
- Any investigative activity during the collection of volatile data must be captured as part of the process. Which combination of steps should the security engineer take to meet these requirements with the LEAST operational overhead? (Select THREE.)

- A. Gather any relevant metadata for the compromised EC2 instance
- B. Enable termination protection
- C. Isolate the instance by updating the instance's security groups to restrict access
- D. Detach the instance from any Auto Scaling groups that the instance is a member of
- E. Deregister the instance from any Elastic Load Balancing (ELB) resources.
- F. Gather any relevant metadata for the compromised EC2 instance
- G. Enable termination protection
- H. Move the instance to an isolation subnet that denies all source and destination traffic
- I. Associate the instance with the subnet to restrict access
- J. Detach the instance from any Auto Scaling groups that the instance is a member of
- K. Deregister the instance from any Elastic Load Balancing (ELB) resources.
- L. Use Systems Manager Run Command to invoke scripts that collect volatile data.
- M. Establish a Linux SSH or Windows Remote Desktop Protocol (RDP) session to the compromised EC2 instance to invoke scripts that collect volatile data.
- N. Create a snapshot of the compromised EC2 instance's EBS volume for follow-up investigation
- O. Tag the instance with any relevant metadata and incident ticket information.
- P. Create a Systems Manager State Manager association to generate an EBS volume snapshot of the compromised EC2 instance
- Q. Tag the instance with any relevant metadata and incident ticket information.

**Answer:** ACE

**NEW QUESTION 53**

A company stores sensitive documents in Amazon S3 by using server-side encryption with an IAM Key Management Service (IAM KMS) CMK. A new requirement mandates that the CMK that is used for these documents can be used only for S3 actions.

Which statement should the company add to the key policy to meet this requirement?

A)

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:CallerAccount": "s3.amazonaws.com"
    }
  }
}
```

B)

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:ViaService": "kms.*amazonaws.com"
    }
  }
}
```

- A. Option A
- B. Option B

**Answer:** A

**NEW QUESTION 57**

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

Please select:



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

**Answer:** A

**Explanation:**

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

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

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

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

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

**NEW QUESTION 58**

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 59**

An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "BlockAnyAccessUnlessSignedInWithMFA",
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {
          "aws:MultiFactorAuthPresent": false
        }
      }
    }
  ]
}
```

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI. What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

- A. Change the value of aws:MultiFactorAuthPresent to true.
- B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication--serial-number and --token-code parameter
- C. Use these resulting values to make API/CLI calls.
- D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
- E. Create a role and enforce multi-factor authentication in the role trust polic



- F. Instruct users to run the sts assume-role CLI command and pass --serial-number and --token-code parameter
- G. Store the resulting values in environment variable
- H. Add sts:AssumeRole to NotAction in the policy.

**Answer: B**

**Explanation:**

The correct answer is B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication --serial-number and --token-code parameters. Use these resulting values to make API/CLI calls.

According to the AWS documentation<sup>1</sup>, the aws sts get-session-token CLI command returns a set of temporary credentials for an AWS account or IAM user. The credentials consist of an access key ID, a secret access key, and a security token. These credentials are valid for the specified duration only. The session duration for IAM users can be between 15 minutes and 36 hours, with a default of 12 hours.

You can use the --serial-number and --token-code parameters to provide the MFA device serial number and the MFA code from the device. The MFA device must be associated with the user who is making the

get-session-token call. If you do not provide these parameters when your IAM user or role has a policy that requires MFA, you will receive an Access Denied error. The temporary security credentials that are returned by the get-session-token command can then be used to make subsequent API or CLI calls that require MFA authentication. You can use environment variables or a profile in your AWS CLI configuration file to specify the temporary credentials.

Therefore, this solution will resolve the problem of users being unable to perform EC2 commands using the AWS CLI, while still enforcing MFA.

The other options are incorrect because:

- A. Changing the value of aws:MultiFactorAuthPresent to true will not work, because this is a condition key that is evaluated by AWS when a request is made. You cannot set this value manually in your policy or request. You must provide valid MFA information to AWS for this condition key to be true.
- C. Implementing federated API/CLI access using SAML 2.0 may work, but it requires more operational effort than using the get-session-token command. You would need to configure a SAML identity provider and trust relationship with AWS, and use a custom SAML client to request temporary credentials from AWS STS. This solution may also introduce additional security risks if the identity provider is compromised.
- D. Creating a role and enforcing MFA in the role trust policy may work, but it also requires more operational effort than using the get-session-token command. You would need to create a role for each user or group that needs to perform EC2 commands, and specify a trust policy that requires MFA. You would also need to grant the users permission to assume the role, and instruct them to use the sts assume-role command instead of the get-session-token command.

References:

1: get-session-token — AWS CLI Command Reference

**NEW QUESTION 64**

A Security Architect has been asked to review an existing security architecture and identify why the application servers cannot successfully initiate a connection to the database servers. The following summary describes the architecture:

- \* 1 An Application Load Balancer, an internet gateway, and a NAT gateway are configured in the public subnet
  - \* 2. Database, application, and web servers are configured on three different private subnets.
  - \* 3 The VPC has two route tables: one for the public subnet and one for all other subnets The route table for the public subnet has a 0 0 0 0/0 route to the internet gateway The route table for all other subnets has a 0 0.0.0/0 route to the NAT gateway. All private subnets can route to each other
  - \* 4 Each subnet has a network ACL implemented that limits all inbound and outbound connectivity to only the required ports and protocols
  - \* 5 There are 3 Security Groups (SGs) database application and web Each group limits all inbound and outbound connectivity to the minimum required
- Which of the following accurately reflects the access control mechanisms the Architect should verify<sup>1</sup>?

- A. Outbound SG configuration on database servers Inbound SG configuration on application servers inbound and outbound network ACL configuration on the database subnet Inbound and outbound network ACL configuration on the application server subnet
- B. Inbound SG configuration on database servers Outbound SG configuration on application servers Inbound and outbound network ACL configuration on the database subnet Inbound and outbound network ACL configuration on the application server subnet
- C. Inbound and outbound SG configuration on database servers Inbound and outbound SG configuration on application servers Inbound network ACL configuration on the database subnet Outbound network ACL configuration on the application server subnet
- D. Inbound SG configuration on database servers Outbound SG configuration on application servers Inbound network ACL configuration on the database subnet Outbound network ACL configuration on the application server subnet.

**Answer: A**

**Explanation:**

this is the accurate reflection of the access control mechanisms that the Architect should verify. Access control mechanisms are methods that regulate who can access what resources and how. Security groups and network ACLs are two types of access control mechanisms that can be applied to EC2 instances and subnets. Security groups are stateful, meaning they remember and return traffic that was previously allowed. Network ACLs are stateless, meaning they do not remember or return traffic that was previously allowed. Security groups and network ACLs can have inbound and outbound rules that specify the source, destination, protocol, and port of the traffic. By verifying the outbound security group configuration on database servers, the inbound security group configuration on application servers, and the inbound and outbound network ACL configuration on both the database and application server subnets, the Architect can check if there are any misconfigurations or conflicts that prevent the application servers from initiating a connection to the database servers. The other options are either inaccurate or incomplete for verifying the access control mechanisms.

**NEW QUESTION 68**

A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file. However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.

What should the security engineer do next to resolve the issue?

- A. Add AWS CloudTrail to the trust policy of the EC2 instance
- B. Send the custom logs to CloudTrail instead of CloudWatch.
- C. Add Amazon S3 to the trust policy of the EC2 instance
- D. Configure the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs.
- E. Add Amazon Inspector to the trust policy of the EC2 instance
- F. Use Amazon Inspector instead of the CloudWatch agent to collect the custom logs.
- G. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

**Answer: D**

**Explanation:**

The correct answer is D. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

According to the AWS documentation<sup>1</sup>, the CloudWatch agent is a software agent that you can install on your EC2 instances to collect system-level metrics and logs. To use the CloudWatch agent, you need to attach an IAM role or user to the EC2 instance that grants permissions for the agent to perform actions on your behalf. The CloudWatchAgentServerPolicy is an AWS managed policy that provides the necessary permissions for the agent to write metrics and logs to CloudWatch<sup>2</sup>. By attaching this policy to the EC2 instance role, the security engineer can resolve the issue of CloudWatch not receiving the custom application-security logs.

The other options are incorrect for the following reasons:

- A. Adding AWS CloudTrail to the trust policy of the EC2 instance is not relevant, because CloudTrail is a service that records API activity in your AWS account, not custom application logs<sup>3</sup>. Sending the custom logs to CloudTrail instead of CloudWatch would not meet the requirement of forwarding them to CloudWatch.
- B. Adding Amazon S3 to the trust policy of the EC2 instance is not necessary, because S3 is a storage service that does not require any trust relationship with EC2 instances<sup>4</sup>. Configuring the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs would be an alternative solution, but it would be more complex and costly than using the CloudWatch agent directly.
- C. Adding Amazon Inspector to the trust policy of the EC2 instance is not helpful, because Inspector is a service that scans EC2 instances for software vulnerabilities and unintended network exposure, not custom application logs<sup>5</sup>. Using Amazon Inspector instead of the CloudWatch agent would not meet the requirement of forwarding them to CloudWatch.

References:

1: Collect metrics, logs, and traces with the CloudWatch agent - Amazon CloudWatch 2: CloudWatchAgentServerPolicy - AWS Managed Policy 3: What Is AWS CloudTrail? - AWS CloudTrail 4: Amazon S3 FAQs - Amazon Web Services 5: Automated Software Vulnerability Management - Amazon Inspector - AWS

## NEW QUESTION 69

A company uses an Amazon S3 bucket to store reports Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client-specified IAM Key Management Service (IAM KMS) CMK owned by the same account as the S3 bucket. The IAM account number is 111122223333, and the bucket name is report bucket. The company's security specialist must write the S3 bucket policy to ensure the mandate can be implemented

Which statement should the security specialist include in the policy?

- A. 

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::reportbucket/*",
  "Condition": {
    "StringEquals": {
      "s3:x-amz-server-side-encryption": "AES256"
    }
  }
}
```
- B. 

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::reportbucket/*",
  "Condition": {
    "StringNotLike": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
    }
  }
}
```
- C. 

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::reportbucket/*",
  "Condition": {
    "StringNotLike": {
      "s3:x-amz-server-side-encryption": "aws:kms"
    }
  }
}
```
- D. 

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::reportbucket/*",
  "Condition": {
    "StringNotLikeIfExists": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:*:111122223333:key/*"
    }
  }
}
```
- E. Option A  
 F. Option B  
 G. Option C  
 H. Option D

Answer: D

## NEW QUESTION 70

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

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 75**

A corporation is preparing to acquire several companies. A Security Engineer must design a solution to ensure that newly acquired IAM accounts follow the corporation's security best practices. The solution should monitor each Amazon S3 bucket for unrestricted public write access and use IAM managed services. What should the Security Engineer do to meet these requirements?

- A. Configure Amazon Macie to continuously check the configuration of all S3 buckets.
- B. Enable IAM Config to check the configuration of each S3 bucket.
- C. Set up IAM Systems Manager to monitor S3 bucket policies for public write access.
- D. Configure an Amazon EC2 instance to have an IAM role and a cron job that checks the status of all S3 buckets.

**Answer:** C

**Explanation:**

because this is a solution that can monitor each S3 bucket for unrestricted public write access and use IAM managed services. S3 is a service that provides object storage in the cloud. Systems Manager is a service that helps you automate and manage your AWS resources. You can use Systems Manager to monitor S3 bucket policies for public write access by using a State Manager association that runs a predefined document called AWS-FindS3BucketWithPublicWriteAccess. This document checks each S3 bucket in an account and reports any bucket that has public write access enabled. The other options are either not suitable or not feasible for meeting the requirements.

**NEW QUESTION 79**

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

The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team. Which combination of solutions will meet these requirements? (Select TWO.)

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

**Answer:** AE

**Explanation:**

The combination of solutions that will meet the requirements are:

- A. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities. This is a valid solution because it allows the security team to access the workload AWS account and instances using a local IAM user that does not depend on SAML federation. It also enables logging and monitoring of the break glass user activities using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon EventBridge123.
  - E. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic. This is a valid solution because it allows the security team to access the workload instances without opening any inbound ports or managing SSH keys or bastion hosts. It also enables logging and notification of the break glass user activities using AWS CloudTrail, Session Manager, and Amazon SNS456.
- The other options are incorrect because:
- B. Creating a break glass EC2 key pair for the AWS account and providing it to the security team is not a valid solution, because it requires opening inbound ports on the instances and managing SSH keys, which increases the security risk and complexity7.
  - C. Creating a break glass IAM role for the account and allowing security team members to perform the AssumeRoleWithSAML operation is not a valid solution, because it still depends on SAML federation, which might not work in case of SAML errors8.
  - D. Creating a local individual break glass IAM user on the operating system level of each workload instance and configuring unrestricted security groups on the instances to grant access to the break glass IAM users is not a valid solution, because it requires opening inbound ports on the instances and managing multiple local users, which increases the security risk and complexity9.



#### References:

1: Creating an IAM User in Your AWS Account 2: Creating a Trail - AWS CloudTrail 3: Using Amazon EventBridge with AWS CloudTrail 4: Setting up Session Manager - AWS Systems Manager 5: Logging Session Manager sessions - AWS Systems Manager 6: Amazon Simple Notification Service 7: Connecting to your Linux instance using SSH - Amazon Elastic Compute Cloud 8: AssumeRoleWithSAML - AWS Security Token Service 9: IAM Users - AWS Identity and Access Management

#### NEW QUESTION 82

A security team is developing an application on an Amazon EC2 instance to get objects from an Amazon S3 bucket. All objects in the S3 bucket are encrypted with an AWS Key Management Service (AWS KMS) customer managed key. All network traffic for requests that are made within the VPC is restricted to the AWS infrastructure. This traffic does not traverse the public internet.

The security team is unable to get objects from the S3 bucket Which factors could cause this issue? (Select THREE.)

- A. The IAM instance profile that is attached to the EC2 instance does not allow the s3 ListBucket action to the S3; bucket in the AWS accounts.
- B. The IAM instance profile that is attached to the EC2 instance does not allow the s3 ListParts action to the S3; bucket in the AWS accounts.
- C. The KMS key policy that encrypts the object in the S3 bucket does not allow the kms; ListKeys action to the EC2 instance profile ARN.
- D. The KMS key policy that encrypts the object in the S3 bucket does not allow the kms Decrypt action to the EC2 instance profile ARN.
- E. The security group that is attached to the EC2 instance is missing an outbound rule to the S3 managed prefix list over port 443.
- F. The security group that is attached to the EC2 instance is missing an inbound rule from the S3 managed prefix list over port 443.

**Answer:** ADE

#### Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html>

To get objects from an S3 bucket that are encrypted with a KMS customer managed key, the security team needs to have the following factors in place:

- The IAM instance profile that is attached to the EC2 instance must allow the s3:GetObject action to the S3 bucket or object in the AWS account. This permission is required to read the object from S3. Option A is incorrect because it specifies the s3:ListBucket action, which is only required to list the objects in the bucket, not to get them.
- The KMS key policy that encrypts the object in the S3 bucket must allow the kms:Decrypt action to the EC2 instance profile ARN. This permission is required to decrypt the object using the KMS key. Option D is correct.
- The security group that is attached to the EC2 instance must have an outbound rule to the S3 managed prefix list over port 443. This rule is required to allow HTTPS traffic from the EC2 instance to S3 within the AWS infrastructure. Option E is correct. Option B is incorrect because it specifies the s3:ListParts action, which is only required for multipart uploads, not for getting objects. Option C is incorrect because it specifies the kms:ListKeys action, which is not required for getting objects. Option F is incorrect because it specifies an inbound rule from the S3 managed prefix list, which is not required for getting objects. Verified References:
- <https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html>
- <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html>

#### NEW QUESTION 85

A company hosts business-critical applications on Amazon EC2 instances in a VPC. The VPC uses default DHCP options sets. A security engineer needs to log all DNS queries that internal resources make in the VPC. The security engineer also must create a list of the most common DNS queries over time.

Which solution will meet these requirements?

- A. Install the Amazon CloudWatch agent on each EC2 instance in the VP
- B. Use the CloudWatch agent to stream the DNS query logs to an Amazon CloudWatch Logs log grou
- C. Use CloudWatch metric filters to automatically generate metrics that list the most common DNS queries.
- D. Install a BIND DNS server in the VP
- E. Create a bash script to list the DNS request number of common DNS queries from the BIND logs.
- F. Create VPC flow logs for all subnets in the VP
- G. Stream the flow logs to an Amazon CloudWatch Logs log grou
- H. Use CloudWatch Logs Insights to list the most common DNS queries for the log group in a custom dashboard.
- I. Configure Amazon Route 53 Resolver query loggin
- J. Add an Amazon CloudWatch Logs log group as the destinatio
- K. Use Amazon CloudWatch Contributor Insights to analyze the data and create time series that display the most common DNS queries.

**Answer:** D

#### Explanation:

<https://aws.amazon.com/blogs/aws/log-your-vpc-dns-queries-with-route-53-resolver-query-logs/>

#### NEW QUESTION 89

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

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

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

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

**Answer:** BCF



**NEW QUESTION 93**

A company wants to monitor the deletion of AWS Key Management Service (AWS KMS) customer managed keys. A security engineer needs to create an alarm that will notify the company before a KMS key is deleted. The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch. What should the security engineer do next to meet these requirements?

- A. Specify the deletion time of the key material during KMS key creatio
- B. Create a custom AWS Config rule to assess the key's scheduleddeletio
- C. Configure the rule to trigger upon a configuration chang
- D. Send a message to an Amazon Simple Notification Service (Amazon SNS) topic if the key is scheduled for deletion.
- E. Create an Amazon EventBridge rule to detect KMS API calls of DeleteAlia
- F. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the compan
- G. Add the Lambda function as the target of the EventBridge rule.
- H. Create an Amazon EventBridge rule to detect KMS API calls of DisableKey and ScheduleKeyDeletion.Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the compan
- I. Add the Lambda function as the target of the EventBridge rule.
- J. Create an Amazon Simple Notification Service (Amazon SNS) policy to detect KMS API calls of RevokeGrant and ScheduleKeyDeletion.Create an AWS Lambda function to generate the alarm and send the notification to the compan
- K. Add the Lambda function as the target of the SNS policy.

**Answer:** C

**Explanation:**

The AWS documentation states that you can create an Amazon EventBridge rule to detect KMS API calls of DisableKey and ScheduleKeyDeletion. You can then create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company. You can add the Lambda function as the target of the EventBridge rule. This method will meet the requirements.

References: : AWS KMS Developer Guide

**NEW QUESTION 95**

A company that uses AWS Organizations wants to see AWS Security Hub findings for many AWS accounts and AWS Regions. Some of the accounts are in the company's organization, and some accounts are in organizations that the company manages for customers. Although the company can see findings in the Security Hub administrator account for accounts in the company's organization, there are no findings from accounts in other organizations. Which combination of steps should the company take to see findings from accounts that are outside the organization that includes the Security Hub administrator account? (Select TWO.)

- A. Use a designated administration account to automatically set up member accounts.
- B. Create the AWS Service Role ForSecurrty Hub service-linked rote for Security Hub.
- C. Send an administration request from the member accounts.
- D. Enable Security Hub for all member accounts.
- E. Send invitations to accounts that are outside the company's organization from the Security Hub administrator account.

**Answer:** CE

**Explanation:**

To see Security Hub findings for accounts that are outside the organization that includes the Security Hub administrator account, the following steps are required:

➤ Send invitations to accounts that are outside the company's organization from the Security Hub administrator account. This will allow the administrator account to view and manage findings from those accounts. The administrator account can send invitations by using the Security Hub console, API, or CLI. For more information, see Sending invitations to member accounts.

➤ Send an administration request from the member accounts. This will allow the member accounts to accept the invitation from the administrator account and establish a relationship with it. The member accounts can send administration requests by using the Security Hub console, API, or CLI. For more information, see Sending administration requests.

This solution will enable the company to see Security Hub findings for many AWS accounts and AWS Regions, including accounts that are outside its own organization.

The other options are incorrect because they either do not establish a relationship between the administrator and member accounts (A, B), do not enable Security Hub for all member accounts (D), or do not use a valid service for Security Hub (F).

Verified References:

➤ <https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-member-accounts.html>

**NEW QUESTION 99**

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

Please select:

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

**Answer:** C

**Explanation:**

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

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

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

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

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

#### NEW QUESTION 101

A Network Load Balancer (NLB) target instance is not entering the InService state. A security engineer determines that health checks are failing. Which factors could cause the health check failures? (Select THREE.)

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

**Answer:** ACD

#### NEW QUESTION 102

A company recently had a security audit in which the auditors identified multiple potential threats. These potential threats can cause usage pattern changes such as DNS access peak, abnormal instance traffic, abnormal network interface traffic, and unusual Amazon S3 API calls. The threats can come from different sources and can occur at any time. The company needs to implement a solution to continuously monitor its system and identify all these incoming threats in near-real time. Which solution will meet these requirements?

- A. Enable AWS CloudTrail logs, VPC flow logs, and DNS log
- B. Use Amazon CloudWatch Logs to manage these logs from a centralized account.
- C. Enable AWS CloudTrail logs, VPC flow logs, and DNS log
- D. Use Amazon Macie to monitor these logs from a centralized account.
- E. Enable Amazon GuardDuty from a centralized account
- F. Use GuardDuty to manage AWS CloudTrail logs, VPC flow logs, and DNS logs.
- G. Enable Amazon Inspector from a centralized account
- H. Use Amazon Inspector to manage AWS CloudTrail logs, VPC flow logs, and DNS logs.

**Answer:** C

#### Explanation:

Q: Which data sources does GuardDuty analyze? GuardDuty analyzes CloudTrail management event logs, CloudTrail S3 data event logs, VPC Flow Logs, DNS query logs, and Amazon EKS audit logs. GuardDuty can also scan EBS volume data for possible malware when GuardDuty Malware Protection is enabled and identifies suspicious behavior indicative of malicious software in EC2 instance or container workloads. The service is optimized to consume large data volumes for near real-time processing of security detections. GuardDuty gives you access to built-in detection techniques developed and optimized for the cloud, which are maintained and continuously improved upon by GuardDuty engineering.

#### NEW QUESTION 104

A developer is building a serverless application hosted on AWS that uses Amazon Redshift as a data store. The application has separate modules for readwrite and read-only functionality. The modules need their own database users for compliance reasons. Which combination of steps should a security engineer implement to grant appropriate access? (Select TWO.)

- A. Configure cluster security groups for each application module to control access to database users that are required for read-only and readwrite
- B. Configure a VPC endpoint for Amazon Redshift. Configure an endpoint policy that maps database users to each application module, and allow access to the tables that are required for read-only and read/write
- C. Configure an IAM policy for each module. Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call
- D. Create local database users for each module
- E. Configure an IAM policy for each module. Specify the ARN of an IAM user that allows the GetClusterCredentials API call

**Answer:** A

#### Explanation:

To grant appropriate access to separate modules for read-write and read-only functionality in a serverless application hosted on AWS that uses Amazon Redshift as a data store, a security engineer should configure cluster security groups for each application module to control access to database users that are required for read-only and readwrite, and configure an IAM policy for each module specifying the ARN of an IAM user that allows the GetClusterCredentials API call.

References: : Amazon Redshift - Amazon Web Services : Amazon Redshift - Amazon Web Services : Identity and Access Management - AWS Management Console : AWS Identity and Access Management - AWS Management Console

#### NEW QUESTION 108

A company uses Amazon GuardDuty. The company's security team wants all High severity findings to automatically generate a ticket in a third-party ticketing system through email integration. Which solution will meet this requirement?

- A. Create a verified identity for the third-party ticketing email system in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty finding
- B. Specify the SES identity as the target for the EventBridge rule.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic
- D. Subscribe the third-party ticketing email system to the SNS topic
- E. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty finding
- F. Specify the SNS topic as the target for the EventBridge rule.
- G. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity finding
- H. Export the results of the filter to an Amazon Simple Notification Service (Amazon SNS) topic
- I. Subscribe the third-party ticketing email system to the SNS topic.
- J. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity finding
- K. Create an Amazon Simple Notification Service (Amazon SNS) topic
- L. Subscribe the third-party ticketing email system to the SNS topic
- M. Create an Amazon EventBridge rule that includes an event pattern that matches GuardDuty findings that are selected by the filter
- N. Specify the SNS topic as the target for the EventBridge rule.

**Answer:** B

**Explanation:**

The correct answer is B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SNS topic as the target for the EventBridge rule.

According to the AWS documentation<sup>1</sup>, you can use Amazon EventBridge to create rules that match events from GuardDuty and route them to targets such as Amazon SNS topics. You can use event patterns to filter events based on criteria such as severity, type, or resource. For example, you can create a rule that matches only High severity findings and sends them to an SNS topic that is subscribed by a third-party ticketing email system. This way, you can automate the creation of tickets for High severity findings and notify the security team.

**NEW QUESTION 111**

A company deployed Amazon GuardDuty In the us-east-1 Region. The company wants all DNS logs that relate to the company's Amazon EC2 instances to be inspected. What should a security engineer do to ensure that the EC2 instances are logged?

- A. Use IPv6 addresses that are configured for hostnames.
- B. Configure external DNS resolvers as internal resolvers that are visible only to IAM.
- C. Use IAM DNS resolvers for all EC2 instances.
- D. Configure a third-party DNS resolver with logging for all EC2 instances.

**Answer:** C

**Explanation:**

To ensure that the EC2 instances are logged, the security engineer should do the following:

- Use AWS DNS resolvers for all EC2 instances. This allows the security engineer to use Amazon-provided DNS servers that resolve public DNS hostnames to private IP addresses within their VPC, and that log DNS queries in Amazon CloudWatch Logs.

**NEW QUESTION 115**

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 119**

A company has multiple departments. Each department has its own IAM account. All these accounts belong to the same organization in IAM Organizations.

A large .csv file is stored in an Amazon S3 bucket in the sales department's IAM account. The company wants to allow users from the other accounts to access the .csv file's content through the combination of IAM Glue and Amazon Athena. However, the company does not want to allow users from the other accounts to access other files in the same folder.

Which solution will meet these requirements?

- A. Apply a user policy in the other accounts to allow IAM Glue and Athena to access the .csv file.
- B. Use S3 Select to restrict access to the .csv file.
- C. In IAM Glue Data Catalog, use S3 Select as the source of the IAM Glue database.
- D. Define an IAM Glue Data Catalog resource policy in IAM Glue to grant cross-account S3 object access to the .csv file.
- E. Grant IAM Glue access to Amazon S3 in a resource-based policy that specifies the organization as the principal.

**Answer:** A

**NEW QUESTION 123**

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 gatewa
- 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 125**

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 rol
- 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 tim
- E. Review the IAM Access Advisor tab for all federated role
- 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 even
- 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 127**

A startup company is using a single AWS account that has resources in a single AWS Region. A security engineer configures an AWS Cloud Trail trail in the same Region to deliver log files to an Amazon S3 bucket by using the AWS CLI.

Because of expansion, the company adds resources in multiple Regions. The security engineer notices that the logs from the new Regions are not reaching the S3 bucket.

What should the security engineer do to fix this issue with the LEAST amount of operational overhead?

- A. Create a new CloudTrail trail
- B. Select the new Regions where the company added resources.
- C. Change the S3 bucket to receive notifications to track all actions from all Regions.
- D. Create a new CloudTrail trail that applies to all Regions.
- E. Change the existing CloudTrail trail so that it applies to all Regions.

**Answer:** D

**Explanation:**

The correct answer is D. Change the existing CloudTrail trail so that it applies to all Regions.

According to the AWS documentation<sup>1</sup>, you can configure CloudTrail to deliver log files from multiple Regions to a single S3 bucket for a single account. To change an existing single-Region trail to log in all Regions, you must use the AWS CLI and add the `--is-multi-region-trail` option to the `update-trail` command<sup>2</sup>. This will ensure that you log global service events and capture all management event activity in your account.

Option A is incorrect because creating a new CloudTrail trail for each Region will incur additional costs and increase operational overhead. Option B is incorrect because changing the S3 bucket to receive notifications will not affect the delivery of log files from other Regions. Option C is incorrect because creating a new CloudTrail trail that applies to all Regions will result in duplicate log files for the original Region and also incur additional costs.

**NEW QUESTION 128**

A security engineer is checking an AWS CloudFormation template for vulnerabilities. The security engineer finds a parameter that has a default value that exposes an application's API key in plaintext. The parameter is referenced several times throughout the template. The security engineer must replace the parameter while maintaining the ability to reference the value in the template. Which solution will meet these requirements in the MOST secure way?

{resolve:s3:MyBucketName:MyObjectName}}.



- A. Store the API key value as a SecureString parameter in AWS Systems Manager Parameter Store
- B. In the template, replace all references to the value with `{{resolve:ssm:MySSMParameterName:1}}`.
- C. Store the API key value in AWS Secrets Manager
- D. In the template, replace all references to the value with `{ {resolve:secretsmanager:MySecretId:SecretString}}`.
- E. Store the API key value in Amazon DynamoDB
- F. In the template, replace all references to the value with `{{resolve:dynamodb:MyTableName:MyPrimaryKey}}`.
- G. Store the API key value in a new Amazon S3 bucket
- H. In the template, replace all references to the value with `{`

**Answer: B**

**Explanation:**

The correct answer is B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with

`{{resolve:secretsmanager:MySecretId:SecretString}}`.

This answer is correct because AWS Secrets Manager is a service that helps you protect secrets that are needed to access your applications, services, and IT resources. You can store and manage secrets such as database credentials, API keys, and other sensitive data in Secrets Manager. You can also use Secrets Manager to rotate, manage, and retrieve your secrets throughout their lifecycle<sup>1</sup>. Secrets Manager integrates with AWS CloudFormation, which allows you to reference secrets from your templates using the

`{{resolve:secretsmanager:...}}` syntax<sup>2</sup>. This way, you can avoid exposing your secrets in plaintext and still use them in your resources.

The other options are incorrect because:

➤ A. Storing the API key value as a SecureString parameter in AWS Systems Manager Parameter Store is not a solution, because AWS CloudFormation does not support references to SecureString parameters. This means that you cannot use the `{{resolve:ssm:...}}` syntax to retrieve encrypted parameter values from Parameter Store<sup>3</sup>. You would have to use a custom resource or a Lambda function to decrypt the parameter value, which adds complexity and overhead to your template.

➤ C. Storing the API key value in Amazon DynamoDB is not a solution, because AWS CloudFormation does not support references to DynamoDB items. This means that you cannot use the `{{resolve:dynamodb:...}}` syntax to retrieve item values from DynamoDB tables<sup>4</sup>. You would have to use a custom resource or a Lambda function to query the DynamoDB table, which adds complexity and overhead to your template.

➤ D. Storing the API key value in a new Amazon S3 bucket is not a solution, because AWS CloudFormation does not support references to S3 objects. This means that you cannot use the `{{resolve:s3:...}}` syntax to retrieve object values from S3 buckets<sup>5</sup>. You would have to use a custom resource or a Lambda function to download the object from S3, which adds complexity and overhead to your template.

References:

1: What is AWS Secrets Manager? 2: Referencing AWS Secrets Manager secrets from Parameter Store parameters 3: Using dynamic references to specify template values 4: Amazon DynamoDB 5: Amazon Simple Storage Service (S3)

**NEW QUESTION 133**

A Security Engineer is troubleshooting an issue with a company's custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events to an Amazon SNS topic. All logs are encrypted at rest using an IAM KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.

The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No logs are being received.

What should the Security Engineer do to troubleshoot this issue?

A) Add the following statement to the IAM managed CMKs:

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": ["sns.amazonaws.com", "sqs.amazonaws.com", "s3.amazonaws.com"]
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

B)

Add the following statement to the CMK key policy:

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": "sns.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

C)

Add the following statement to the CMK key policy:

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": "sns.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": "sns.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

D)

Add the following statement to the CMK key policy:

```
{
  "Sid": "Allow Amazon SNS to use this key",
  "Effect": "Allow",
  "Principal": {
    "Service": "sns.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

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

**Answer: D**

#### NEW QUESTION 135

A security engineer has enabled IAM Security Hub in their IAM account, and has enabled the Center for internet Security (CIS) IAM Foundations compliance standard. No evaluation results on compliance are returned in the Security Hub console after several hours. The engineer wants to ensure that Security Hub can evaluate their resources for CIS IAM Foundations compliance.

Which steps should the security engineer take to meet these requirements?

- A. Add full Amazon Inspector IAM permissions to the Security Hub service role to allow it to perform the CIS compliance evaluation
- B. Ensure that IAM Trusted Advisor Is enabled in the account and that the Security Hub service role has permissions to retrieve the Trusted Advisor security-related recommended actions
- C. Ensure that IAM Config
- D. is enabled in the account, and that the required IAM Config rules have been created for the CIS compliance evaluation
- E. Ensure that the correct trail in IAM CloudTrail has been configured for monitoring by Security Hub and that the Security Hub service role has permissions to perform the GetObject operation on CloudTrails Amazon S3 bucket

**Answer: C**

#### Explanation:

To ensure that Security Hub can evaluate their resources for CIS AWS Foundations compliance, the security engineer should do the following:

- Ensure that AWS Config is enabled in the account. This is a service that enables continuous assessment and audit of your AWS resources for compliance.
- Ensure that the required AWS Config rules have been created for the CIS compliance evaluation. These are rules that represent your desired configuration settings for specific AWS resources or for an entire AWS account.

#### NEW QUESTION 136

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

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

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

**Answer: CE**

#### 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 139

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

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

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

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

**Answer: B**

#### Explanation:

This option suggests updating the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule, replacing the security group with a new one that only allows connections from a diagnostics security group, and launching a new EC2 instance with diagnostic tools to investigate the suspicious instance. This option will immediately mitigate the attack and provide the necessary tools for investigation.

#### NEW QUESTION 143

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

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

**Answer: A**

#### NEW QUESTION 145

A team is using AWS Secrets Manager to store an application database password. Only a limited number of IAM principals within the account can have access to the secret. The principals who require access to the secret change frequently. A security engineer must create a solution that maximizes flexibility and scalability. Which solution will meet these requirements?

- A. Use a role-based approach by creating an IAM role with an inline permissions policy that allows access to the secret.
- B. Update the IAM principals in the role trust policy as required.
- C. Deploy a VPC endpoint for Secrets Manager.
- D. Create and attach an endpoint policy that specifies the IAM principals that are allowed to access the secret.
- E. Update the list of IAM principals as required.
- F. Use a tag-based approach by attaching a resource policy to the secret.
- G. Apply tags to the secret and the IAM principal.
- H. Use the aws:PrincipalTag and aws:ResourceTag IAM condition keys to control access.
- I. Use a deny-by-default approach by using IAM policies to deny access to the secret explicitly.
- J. Attach the policies to an IAM group.
- K. Add all IAM principals to the IAM group.
- L. Remove principals from the group when they need access.
- M. Add the principals to the group again when access is no longer allowed.

**Answer: C**

#### NEW QUESTION 150

A company is using AWS Organizations to manage multiple accounts. The company needs to allow an IAM user to use a role to access resources that are in another organization's AWS account.

Which combination of steps must the company perform to meet this requirement? (Select TWO.)



- A. Create an identity policy that allows the sts: AssumeRole action in the AWS account that contains the resource
- B. Attach the identity policy to the IAM user.
- C. Ensure that the sts: AssumeRole action is allowed by the SCPs of the organization that owns the resources that the IAM user needs to access.
- D. Create a role in the AWS account that contains the resource
- E. Create an entry in the role's trust policy that allows the IAM user to assume the rol
- F. Attach the trust policy to the role.
- G. Establish a trust relationship between the IAM user and the AWS account that contains the resources.
- H. Create a role in the IAM user's AWS account
- I. Create an identity policy that allows the sts: AssumeRole actio
- J. Attach the identity policy to the role.

**Answer:** BC

**Explanation:**

To allow cross-account access to resources using IAM roles, the following steps are required:

- Create a role in the AWS account that contains the resources (the trusting account) and specify the AWS account that contains the IAM user (the trusted account) as a trusted entity in the role's trust policy. This allows users from the trusted account to assume the role and access resources in the trusting account.
- Ensure that the IAM user has permission to assume the role in their own AWS account. This can be done by creating an identity policy that allows the sts:AssumeRole action and attaching it to the IAM user or their group.
- Ensure that there are no service control policies (SCPs) in the organization that owns the resources that deny or restrict access to the sts:AssumeRole action or the role itself. SCPs are applied to all accounts in an organization and can override any permissions granted by IAM policies.

Verified References:

- <https://repost.aws/knowledge-center/cross-account-access-iam>
- [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_accounts\\_access.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html)
- [https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\\_cross-account-with-roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html)

**NEW QUESTION 151**

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 156**

A company accidentally deleted the private key for an Amazon Elastic Block Store (Amazon EBS)-backed Amazon EC2 instance. A security engineer needs to regain access to the instance.

Which combination of steps will meet this requirement? (Choose two.)

- A. Stop the instanc
- B. Detach the root volum
- C. Generate a new key pair.
- D. Keep the instance runnin
- E. Detach the root volum
- F. Generate a new key pair.
- G. When the volume is detached from the original instance, attach the volume to another instance as a data volum
- H. Modify the authorized\_keys file with a new public ke
- I. Move the volume back to the original instanc
- J. Start the instance.
- K. When the volume is detached from the original instance, attach the volume to another instance as a data volum
- L. Modify the authorized\_keys file with a new private ke
- M. Move the volume back to the original instanc
- N. Start the instance.
- O. When the volume is detached from the original instance, attach the volume to another instance as a data volum
- P. Modify the authorized\_keys file with a new public ke
- Q. Move the volume back to the original instance that is running.

**Answer:** AC

**Explanation:**

If you lose the private key for an EBS-backed instance, you can regain access to your instance. You must stop the instance, detach its root volume and attach it to another instance as a data volume, modify the authorized\_keys file with a new public key, move the volume back to the original instance, and restart the instance.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#replacing>

**NEW QUESTION 158**

During a manual review of system logs from an Amazon Linux EC2 instance, a Security Engineer noticed that there are sudo commands that were never properly



alerted or reported on the Amazon CloudWatch Logs agent  
Why were there no alerts on the sudo commands?

- A. There is a security group blocking outbound port 80 traffic that is preventing the agent from sending the logs
- B. The IAM instance profile on the EC2 instance was not properly configured to allow the CloudWatchLogs agent to push the logs to CloudWatch
- C. CloudWatch Logs status is set to ON versus SECURE, which prevents it from pulling in OS security event logs
- D. The VPC requires that all traffic go through a proxy, and the CloudWatch Logs agent does not support a proxy configuration.

**Answer:** B

**Explanation:**

the reason why there were no alerts on the sudo commands. Sudo commands are commands that allow a user to execute commands as another user, usually the superuser or root. CloudWatch Logs agent is a software agent that can send log data from an EC2 instance to CloudWatch Logs, a service that monitors and stores log data. The CloudWatch Logs agent needs an IAM instance profile, which is a container for an IAM role that allows applications running on an EC2 instance to make API requests to AWS services. If the IAM instance profile on the EC2 instance was not properly configured to allow the CloudWatch Logs agent to push the logs to CloudWatch, then there would be no alerts on the sudo commands. The other options are either irrelevant or invalid for explaining why there were no alerts on the sudo commands.

**NEW QUESTION 160**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-Security-Specialty Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-Certified-Security-Specialty Product From:

<https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/>

## Money Back Guarantee

### **AWS-Certified-Security-Specialty Practice Exam Features:**

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