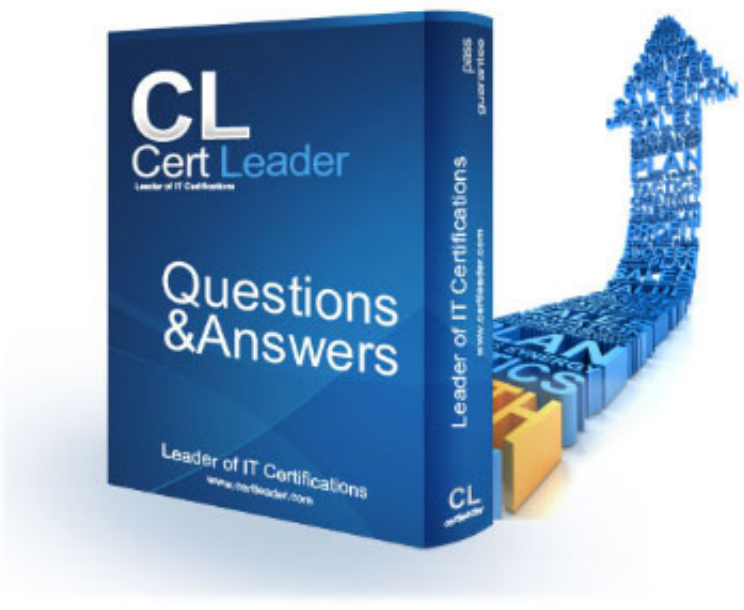
AWS-Certified-Security-Specialty Dumps

Amazon AWS Certified Security - Specialty

https://www.certleader.com/AWS-Certified-Security-Specialty-dumps.html



NEW QUESTION 1
A security engineer wants to use Amazon Simple Notification Service (Amazon SNS) to send email alerts to a company's security team for Amazon GuardDuty findings
that have a High severity level. The security engineer also wants to deliver these findings to a visualization tool for further examination.
Which solution will meet these requirements?

A. Set up GuardDuty to send notifications to an Amazon CloudWatch alarm with two targets in CloudWatc
B. From CloudWatch, stream the findings through Amazon Kinesis Data Streams into an Amazon OpenSearch Service domain as the first target for deliver
C. Use Amazon QuickSight to visualize the finding
D. Use OpenSearch queries for further analysi
E. Deliver email alerts to the security team by configuring an SNS topic as a second target for the CloudWatch alar
F. Use event pattern matching with an Amazon EventBridge event rule to send only High severity findings in the alerts.
G. Set up GuardDuty to send notifications to AWS CloudTrail with two targets in CloudTrai
H. From CloudTrail, stream the findings through Amazon Kinesis Data Firehose into an Amazon OpenSearch Service domain as the first target for deliver
I. Use OpenSearch Dashboards to visualize the finding
J. Use OpenSearch queries for further analysi
K. Deliver email alerts to the security team by configuring an SNS topic as a second target for CloudTrai
L. Use event pattern matching with a CloudTrail event rule to send only High severity findings in the alerts.
M. Set up GuardDuty to send notifications to Amazon EventBridge with two target
N. From EventBridge, stream the findings through Amazon Kinesis Data Firehose into an Amazon OpenSearch Service domain as the first target for deliver
O. Use OpenSearch Dashboards to visualize the finding
P. Use OpenSearch queries for further analysi
Q. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridg
R. Use event pattern matching with an EventBridge event rule to send only High severity findings in the alerts.
S. Set up GuardDuty to send notifications to Amazon EventBridge with two target
T. From EventBridge, stream the findings through Amazon Kinesis Data Streams into an Amazon OpenSearch Service domain as the first target for deliver
. Use Amazon QuickSight to visualize the finding
. Use OpenSearch queries for further analysi
. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridg
. Use event pattern matching with an EventBridge event rule to send only High severity findings in the alerts.

Answer: C

NEW QUESTION 2
A Security Engineer is asked to update an AWS CloudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the Security Engineer receives the following error message: `There is a problem with the bucket policy.` What will enable the Security Engineer to save the change?

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

Answer: C

Explanation:
The correct answer is C. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
According to the AWS documentation1, a bucket policy is a resource-based policy that you can use to grant access permissions to your Amazon S3 bucket and the objects in it. Only the bucket owner can associate a policy with a bucket. The permissions attached to the bucket apply to all of the objects in the bucket that are owned by the bucket owner.
When you create a trail in CloudTrail, you can specify an existing S3 bucket or create a new one to store your log files. CloudTrail automatically creates a bucket policy for your S3 bucket that grants CloudTrail write-only access to deliver log files to your bucket. The bucket policy also grants read-only access to AWS services that you can use to view and analyze your log data, such as Amazon Athena, Amazon CloudWatch Logs, and Amazon QuickSight.
If you want to update the log file prefix for an existing trail, you must also update the existing bucket policy in the S3 console with the new log file prefix. The log file prefix is part of the resource ARN that identifies the objects in your bucket that CloudTrail can access. If you don’t update the bucket policy with the new log file prefix, CloudTrail will not be able to deliver log files to your bucket, and you will receive an error message when you try to save the change in the CloudTrail console.
The other options are incorrect because:

- A. Creating a new trail with the updated log file prefix, and then deleting the original trail is not necessary and may cause data loss or inconsistency. You can simply update the existing trail and its associated bucket policy with the new log file prefix.
- B. Updating the existing bucket policy in the S3 console to allow the Security Engineer’s Principal to perform PutBucketPolicy is not relevant to this issue. The PutBucketPolicy action allows you to create or replace a policy on a bucket, but it does not affect CloudTrail’s ability to deliver log files to your bucket. You still need to update the existing bucket policy with the new log file prefix.
- D. Updating the existing bucket policy in the S3 console to allow the Security Engineer’s Principal to perform GetBucketPolicy is not relevant to this issue. The GetBucketPolicy action allows you to retrieve a policy on a bucket, but it does not affect CloudTrail’s ability to deliver log files to your bucket. You still need to update the existing bucket policy with the new log file prefix.

References:
1: Using bucket policies - Amazon Simple Storage Service

NEW QUESTION 3
A security engineer is creating an AWS Lambda function. The Lambda function needs to use a role that is named LambdaAuditRole to assume a role that is named AcmeAuditFactoryRole in a different AWS account.
When the code is processed, the following error message appears: "An error oc-curred (AccessDenied) when calling the AssumeRole operation."
Which combination of steps should the security engineer take to resolve this er-ror? (Select TWO.)

A. Ensure that LambdaAuditRole has the sts:AssumeRole permission for Ac-meAuditFactoryRole.
B. Ensure that LambdaAuditRole has the AWSLambdaBasicExecutionRole managed policy attached.
C. Ensure that the trust policy for AcmeAuditFactoryRole allows the sts:AssumeRole action from LambdaAuditRole.
D. Ensure that the trust policy for LambdaAuditRole allows the sts:AssumeRole action from the lambda.amazonaws.com service.
E. Ensure that the sts:AssumeRole API call is being issued to the us-east-I Region endpoint.

Answer: AC

NEW QUESTION 4
A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted The security engineer has configured the integration of IAM CloudTrail with Amazon CloudWatch
What should the security engineer do next to meet this requirement?

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

Answer: A

NEW QUESTION 5
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 m 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 6
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 tu encrypt a 512-byte payload. During load testing, a bug appears |intermittently where AccessDeniedExceptions are occasionally triggered when a user rst attempts to encrypt using the CMK
Which solution should the c0mpany‘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 toke
C. Instruct use 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 operatio
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 7
A company wants to establish separate IAM Key Management Service (IAM KMS) keys to use for different IAM services. The company's security engineer created the following key policy lo allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role:

```
{
    "Version": "2012-10-17",
    "Id": "key-policy-ebs",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/aws-reserved/sso.amazonaws.com/InfrastructureDeployment"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.us-west-2.amazonaws.com"
                }
            }
        }
    ]
}
```

The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key (or other services. Which change to the policy should the security engineer make to resolve these issues?

A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
B. In the policy document, remove the statement Dlock that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.
C. In the statement block that contains the Sid "Allow use of the Key", under the "Condition" block, change the Kms:ViaService value to ec2.us-east-1 .amazonIAM com.
D. In the policy document, add a new statement block that grants the kms:Disable' permission to the security engineer's IAM role.

Answer: C

Explanation:
To resolve the issues, the security engineer should make the following change to the policy:
> In the statement block that contains the Sid “Allow use of the key”, under the “Condition” block, change the Kms:ViaService value to ec2.us-east-1.amazonaws.com. This allows the security engineer to restrict the use of the key to only EC2 service in the us-east-1 region, and prevent other services from using the key.

NEW QUESTION 8
A company has a batch-processing system that uses Amazon S3, Amazon EC2, and AWS Key Management Service (AWS KMS). The system uses two AWS accounts: Account A and Account B.
Account A hosts an S3 bucket that stores the objects that will be processed. The S3 bucket also stores the results of the processing. All the S3 bucket objects are encrypted by a KMS key that is managed in
Account A.
Account B hosts a VPC that has a fleet of EC2 instances that access the S3 buck-et in Account A by using statements in the bucket policy. The VPC was created with DNS hostnames enabled and DNS resolution enabled.
A security engineer needs to update the design of the system without changing any of the system's code. No AWS API calls from the batch-processing EC2 in-stances can travel over the internet.
Which combination of steps will meet these requirements? (Select TWO.)

A. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint,create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.
B. In the Account B VPC, create an interface VPC endpoint for Amazon S3. For the interface VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.
C. In the Account B VPC, create an interface VPC endpoint for AWS KM
D. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS ke
E. Ensure that private DNS is turned on for the endpoint.
F. In the Account B VPC, create an interface VPC endpoint for AWS KM
G. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS ke
H. Ensure that private DNS is turned off for the endpoint.
I. In the Account B VPC, verify that the S3 bucket policy allows the s3:PutObjectAcl action for cross-account us
J. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, and s3:PutObject actions for the S3 bucket.

Answer: BC

NEW QUESTION 9
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 acces
B. Create a new access key pai
C. Add environmental variables to the Lambda function with the ac-cess key ID and secret access ke
D. Modify the Lambda function to use the environmental variables at run time during communication with Amazon S3.
E. Generate an Amazon EC2 key pai
F. Store the private key in AWS Secrets Man-age
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 functio
I. Attach an IAM policy that al-lows access to the S3 bucket.
J. Create an IAM role for the Lambda functio
K. Attach a bucket policy to the S3 bucket to allow access.Specify the function's IAM role as the princi-pal.
L. Create a security grou
M. Attach the security group to the Lambda functio
N. Attach a bucket policy that allows access to the S3 bucket through the se-curity 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 functio
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 functio
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 functio
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 m 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 10
An organization has a multi-petabyte workload that it is moving to Amazon S3, but the CISO is concerned about cryptographic wear-out and the blast radius if a key is compromised. How can the CISO be assured that IAM KMS and Amazon S3 are addressing the concerns? (Select TWO)

A. There is no API operation to retrieve an S3 object in its encrypted form.
B. Encryption of S3 objects is performed within the secure boundary of the KMS service.
C. S3 uses KMS to generate a unique data key for each individual object.
D. Using a single master key to encrypt all data includes having a single place to perform audits and usage validation.
E. The KMS encryption envelope digitally signs the master key during encryption to prevent cryptographic wear-out

Answer: CE

Explanation:
because these are the features that can address the CISO’s concerns about cryptographic wear-out and blast radius. Cryptographic wear-out is a phenomenon that occurs when a key is used too frequently or for too long, which increases the risk of compromise or degradation. Blast radius is a measure of how much damage a compromised key can cause to the encrypted data. S3 uses KMS to generate a unique data key for each individual object, which reduces both cryptographic wear-out and blast radius. The KMS encryption envelope digitally signs the master key during encryption, which prevents cryptographic wear-out by ensuring that only authorized parties can use the master key. The other options are either incorrect or irrelevant for addressing the CISO’s concerns.

NEW QUESTION 12
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 drif
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 proces
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 databas
H. Copy the snapshot and enable snapshot encryption in the proces
I. Restore the database instance from the newly created encrypted snapsho
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 17
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 21
A company is building a data processing application mat uses AWS Lambda functions. The application's Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account
Which solution meets these requirements in the MOST secure way?

A. Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region
B. Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0.0.0.0/0
C. Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group
D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

Answer: C

Explanation:
This solution ensures that the Lambda functions are deployed inside the VPC and can communicate with the Amazon RDS DB instance securely. The security group attached to the Lambda functions only allows
outbound traffic to the VPC CIDR range, and the DB instance security group only allows traffic from the Lambda security group. This solution ensures that the Lambda functions can communicate with the DB instance securely and that the DB instance is not exposed to the public internet.

NEW QUESTION 24
A company in France uses Amazon Cognito with the Cognito Hosted Ul 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 trigge
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 AC
D. Associate the web ACL with the Amazon Cognito user pool.
E. Configure an app client for the application's Amazon Cognito user poo
F. Use the app client ID to validate the requests in the hosted Ul.
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 Ul.

Answer: B

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

NEW QUESTION 26
A company is using Amazon Macie, AWS Firewall Manager, Amazon Inspector, and AWS Shield Advanced in its AWS account. The company wants to receive alerts if a DDoS attack occurs against the account.
Which solution will meet this requirement?

A. Use Macie to detect an active DDoS even
B. Create Amazon CloudWatch alarms that respond to Macie findings.
C. Use Amazon Inspector to review resources and to invoke Amazon CloudWatch alarms for any resources that are vulnerable to DDoS attacks.
D. Create an Amazon CloudWatch alarm that monitors Firewall Manager metrics for an active DDoS event.
E. Create an Amazon CloudWatch alarm that monitors Shield Advanced metrics for an active DDoS event.

Answer: D

Explanation:
This answer is correct because AWS Shield Advanced is a service that provides comprehensive protection
against DDoS attacks of any size or duration. It also provides metrics and reports on the DDoS attack vectors, duration, and size. You can create an Amazon CloudWatch alarm that monitors Shield Advanced metrics such as DDoSAttackBitsPerSecond, DDoSAttackPacketsPerSecond, and DDoSAttackRequestsPerSecond to receive alerts if a DDoS attack occurs against your account.
For more information, see Monitoring AWS Shield Advanced with Amazon CloudWatch and AWS Shield Advanced metrics and alarms.

NEW QUESTION 27
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 31
A company is using an AWS Key Management Service (AWS KMS) AWS owned key in its application to encrypt files in an AWS account The company's security team wants the ability to change to new key material for new files whenever a potential key breach occurs A security engineer must implement a solution that gives the security team the ability to change the key whenever the team wants to do so
Which solution will meet these requirements?

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

Answer: A

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

NEW QUESTION 32
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 33
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 34
A company's Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company IAM account The Security Analyst decides to do this by Improving IAM account root user security.
Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

A. Delete the access keys for the account root user in every account.
B. Create an admin IAM user with administrative privileges and delete the account root user in every account.
C. Implement a strong password to help protect account-level access to the IAM Management Console by the account root user.
D. Enable multi-factor authentication (MFA) on every account root user in all accounts.
E. Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.
F. Attach an IAM role to the account root user to make use of the automated credential rotation in IAM STS.

Answer: ADE

Explanation:
because these are the actions that can improve IAM account root user security. IAM account root user is a user that has complete access to all AWS resources and services in an account. IAM account root user security is a set of best practices that help protect the account root user from unauthorized or accidental use. Deleting the access keys for the account root user in every account can help prevent programmatic access by the account root user, which reduces the risk of compromise or misuse. Enabling MFA on every account root user in all accounts can help add an extra layer of security for console access by requiring a verification code in addition to a password. Creating a custom IAM policy to limit permissions to required actions for the account root user and attaching the policy to the account root user can help enforce the principle of least privilege and restrict the account root user from performing unnecessary or dangerous actions. The other options are either invalid or ineffective for improving IAM account root user security.

NEW QUESTION 37
A development team is attempting to encrypt and decode a secure string parameter from the IAM Systems Manager Parameter Store using an IAM Key Management Service (IAM KMS) CMK. However, each attempt results in an error message being sent to the development team.
Which CMK-related problems possibly account for the error? (Select two.)

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

Answer: AD

Explanation:
https://docs.IAM.amazon.com/kms/latest/developerguide/services-parameter-store.html#parameter-store-cmk-fa

NEW QUESTION 38
A company is designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS Single Sign-On (AWS SSO). The company must implement a solution so that the development teams can use only specific AWS Regions and so that each AWS account allows access to only specific AWS services.
Which solution will meet these requirements with the LEAST operational overhead?

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

Answer: C

Explanation:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_syntax.html#scp-eleme

NEW QUESTION 43
A security engineer recently rotated all IAM access keys in an AWS account. The security engineer then configured AWS Config and enabled the following AWS Config managed rules; mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-key-rotated, and iam-user-unused-credentials-check.
The security engineer notices that all resources are displaying as noncompliant after the IAM GenerateCredentialReport API operation is invoked.
What could be the reason for the noncompliant status?

A. The IAM credential report was generated within the past 4 hours.
B. The security engineer does not have the GenerateCredentialReport permission.
C. The security engineer does not have the GetCredentialReport permission.
D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.

Answer: D

Explanation:
The correct answer is D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours. According to the AWS documentation1, the MaximumExecutionFrequency parameter specifies the maximum frequency with which AWS Config runs evaluations for a rule. For AWS Config managed rules, this value can be one of the following:

- One_Hour
- Three_Hours
- Six_Hours
- Twelve_Hours
- TwentyFour_Hours

If the rule is triggered by configuration changes, it will still run evaluations when AWS Config delivers the configuration snapshot. However, if the rule is triggered periodically, it will not run evaluations more often than the specified frequency.
In this case, the security engineer enabled four AWS Config managed rules that are triggered periodically. Therefore, these rules will only run evaluations every 24 hours, regardless of when the IAM credential report is generated. This means that the resources will display as noncompliant until the next evaluation cycle, which could take up to 24 hours after the IAM access keys are rotated.
The other options are incorrect because:

- A. The IAM credential report can be generated at any time, but it will not affect the compliance status of the resources until the next evaluation cycle of the AWS Config rules.
- B. The security engineer was able to invoke the IAM GenerateCredentialReport API operation, which means they have the GenerateCredentialReport permission. This permission is required to generate a credential report that lists all IAM users in an AWS account and their credential status2.
- C. The security engineer does not need the GetCredentialReport permission to enable or evaluate AWS Config rules. This permission is required to retrieve a credential report that was previously generated by using the GenerateCredentialReport operation2.

References:
1: AWS::Config::ConfigRule - AWS CloudFormation 2: IAM: Generate and retrieve IAM credential reports

NEW QUESTION 45
A company created an IAM account for its developers to use for testing and learning purposes Because MM account will be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.
Developers were Instructed to tag al their instances with a Team tag key and use the team name in the tag value One of the first teams to use this account is Business Intelligence A security engineer needs to develop a highly scalable solution for providing developers with access to the appropriate resources within the

account The security engineer has already created individual IAM roles for each team.
Which additional configuration steps should the security engineer take to complete the task?

A. For each team, create an AM policy similar to the one that fellows Populate the ec2: ResourceTag/Team condition key with a proper team name Attach resulting policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ]
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

B. For each team create an IAM policy similar to the one that follows Populate the IAM TagKeys/Team condition key with a proper team nam
C. Attach the resuming policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

D. Tag each IAM role with a Team lag ke
E. and use the team name in the tag valu
F. Create an IAM policy similar to the one that follows, and attach 4 to all the IAM roles used by developers.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "${aws:PrincipalTag/Team}"
                }
            }
        }
    ]
}
```

G. Tag each IAM role with the Team key, and use the team name in the tag valu
H. Create an IAM policy similar to the one that follows, and it to all the IAM roles used by developers.

Answer: A

NEW QUESTION 49
A security engineer needs to implement a write-once-read-many (WORM) model for data that a company will store in Amazon S3 buckets. The company uses the S3 Standard storage class for all of its S3 buckets. The security engineer must en-sure that objects cannot be overwritten or deleted by any user, including the AWS account root user.
Which solution will meet these requirements?

A. Create new S3 buckets with S3 Object Lock enabled in compliance mod
B. Place objects in the S3 buckets.
C. Use S3 Glacier Vault Lock to attach a Vault Lock policy to new S3 bucket
D. Wait 24 hours to complete the Vault Lock proces
E. Place objects in the S3 buckets.
F. Create new S3 buckets with S3 Object Lock enabled in governance mod
G. Place objects in the S3 buckets.
H. Create new S3 buckets with S3 Object Lock enabled in governance mod
I. Add a legal hold to the S3 bucket
J. Place objects in the S3 buckets.

Answer: A

NEW QUESTION 51
A security team is working on a solution that will use Amazon EventBridge (Amazon CloudWatch Events) to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.
Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event. However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.
The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.
Which solution will meet these requirements?

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

Answer: D

Explanation:
The correct answer is D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets. According to the AWS documentation1, CloudTrail data events are the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities. For example, Amazon S3 object-level API activity (such as GetObject, DeleteObject, and PutObject) is a data event.
By default, trails do not log data events. To record CloudTrail data events, you must explicitly add the
supported resources or resource types for which you want to collect activity. For more information, see Logging data events in the Amazon S3 User Guide2.
In this case, the security team wants EventBridge to watch for the s3:PutObjectAcl API invocation logs from CloudTrail. This API uses the acl subresource to set the access control list (ACL) permissions for a new or existing object in an S3 bucket3. This is a data event that affects the S3 object resource type. Therefore, the security team must enable CloudTrail to monitor data events for read and write operations to S3 buckets in order to invoke an EventBridge event for this API call.
The other options are incorrect because:

- A. Modifying the EventBridge event pattern by selecting Amazon S3 and All Events as the event type will not capture the s3:PutObjectAcl API call, because this is a data event and not a management event. Management events provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations4.
- B. Modifying the EventBridge event pattern by selecting Amazon S3 and Bucket Level Operations as the event type will not capture the s3:PutObjectAcl API call, because this is a data event that affects the S3 object resource type and not the S3 bucket resource type. Bucket level operations are management events that affect the configuration or metadata of an S3 bucket5.
- C. Enabling CloudTrail Insights to identify unusual API activity will not help the security team monitor new S3 objects or changes to any S3 bucket policy or setting that result in public access. CloudTrail Insights helps AWS users identify and respond to unusual activity associated with API calls and API error rates by continuously analyzing CloudTrail management events6. It does not analyze data events or generate EventBridge events.

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

NEW QUESTION 53
A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised. The instance was serving up malware. The analysis of the instance showed that the instance was compromised 35 days ago.
A security engineer must implement a continuous monitoring solution that automatically notifies the company's security team about compromised instances through an email distribution list for high severity findings. The security engineer must implement the solution as soon as possible.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

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

Answer: BCE

NEW QUESTION 54
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 55
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 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 59
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 lo access the .csv We.
B. Use S3 Select to restrict access to the .csv li
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 63
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 Stor
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 Manager1.
* 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 policies2. You can also use the AWS SDK for Java to integrate your application with Secrets Manager3.

NEW QUESTION 66
A company is building an application on IAM that will store sensitive Information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.
What should the security engineer recommend?

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

Answer: C

Explanation:
To protect the sensitive data against any data breach and minimize management overhead, the security engineer should recommend the following solution:

- Enable Amazon RDS encryption to encrypt the database and snapshots. This allows the security engineer to use AWS Key Management Service (AWS KMS) to encrypt data at rest for the database and any backups or replicas.
- Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. This allows the security engineer to use AWS KMS to encrypt data at rest for the EC2 instances and any snapshots or volumes.
- Store the database credentials in AWS Secrets Manager with automatic rotation. This allows the security engineer to encrypt and manage secrets centrally, and to configure automatic rotation schedules for them.
- Set up TLS for the connection to the RDS hosted database. This allows the security engineer to encrypt data in transit between the EC2 instances and the database.

NEW QUESTION 69
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 70
A security engineer needs to see up an Amazon CloudFront distribution for an Amazon S3 bucket that hosts a static website. The security engineer must allow only specified IP addresses to access the website. The security engineer also must prevent users from accessing the website directly by using S3 URLs.
Which solution will meet these requirements?

A. Generate an S3 bucket polic
B. Specify cloudfront amazonaws com as the principa
C. Use the aws Sourcelp condition key to allow access only if the request conies from the specified IP addresses.
D. Create a CloudFront origin access identity (OAl). Create the S3 bucket policy so that only the OAl has acces
E. Create an AWS WAF web ACL and add an IP set rul
F. Associate the web ACL with the CloudFront distribution.
G. Implement security groups to allow only the specified IP addresses access and to restrict S3 bucket access by using the CloudFront distribution.
H. Create an S3 bucket access point to allow access from only the CloudFront distributio
I. Create an AWS WAF web ACL and add an IP set rul
J. Associate the web ACL with the CloudFront distribution.

Answer: B

NEW QUESTION 72
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 75
A company uses AWS Organizations. The company wants to implement short-term cre-dentials for third-party AWS accounts to use to access accounts within the com-pany's organization. Access is for the AWS Management Console and third-party software-as-a-service (SaaS) applications. Trust must be enhanced to prevent two external accounts from using the same credentials. The solution must require the least possible operational effort.
Which solution will meet these requirements?

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

Answer: D

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

sts:ExternalId condition key instead to provide a unique identifier for each external account.

NEW QUESTION 79
A company is using Amazon Elastic Container Service (Amazon ECS) to deploy an application that deals with sensitive data During a recent security audit, the company identified a security issue in which Amazon RDS credentials were stored with the application code In the company's source code repository
A security engineer needs to develop a solution to ensure that database credentials are stored securely and rotated periodically. The credentials should be accessible to the application only The engineer also needs to prevent database administrators from sharing database credentials as plaintext with other teammates. The solution must also minimize administrate overhead
Which solution meets these requirements?

A. Use the IAM Systems Manager Parameter Store to generate database credential
B. Use an IAM profile for ECS tasks to restrict access to database credentials to specific containers only.
C. Use IAM Secrets Manager to store database credential
D. Use an IAM inline policy for ECS tasks to restrict access to database credentials to specific containers only.
E. Use the IAM Systems Manager Parameter Store to store database credential
F. Use IAM roles for ECS tasks to restrict access to database credentials lo specific containers only
G. Use IAM Secrets Manager to store database credential
H. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

Answer: D

Explanation:
To ensure that database credentials are stored securely and rotated periodically, the security engineer should do the following:
> Use AWS Secrets Manager to store database credentials. This allows the security engineer to encrypt and manage secrets centrally, and to configure automatic rotation schedules for them.
> Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only. This allows the security engineer to grant fine-grained permissions to ECS tasks based on their roles, and to avoid sharing credentials as plaintext with other teammates.

NEW QUESTION 84
A company is using IAM Organizations to develop a multi-account secure networking strategy. The company plans to use separate centrally managed accounts for shared services, auditing, and security inspection. The company plans to provide dozens of additional accounts to application owners for production and development environments.
Company security policy requires that all internet traffic be routed through a centrally managed security inspection layer in the security inspection account. A security engineer must recommend a solution that minimizes administrative overhead and complexity.
Which solution meets these requirements?

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

Answer: C

NEW QUESTION 87
A company has enabled Amazon GuardDuty in all AWS Regions as part of its security monitoring strategy. In one of its VPCs, the company hosts an Amazon EC2 instance that works as an FTP server. A high number of clients from multiple locations contact the FTP server. GuardDuty identifies this activity as a brute force attack because of the high number of connections that happen every hour.
The company has flagged the finding as a false positive, but GuardDuty continues to raise the issue. A security engineer must improve the signal-to-noise ratio without compromising the companys visibility of potential anomalous behavior.
Which solution will meet these requirements?

A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed.
B. Add the FTP server to a trusted IP lis
C. Deploy the list to GuardDuty to stop receiving the notifications.
D. Create a suppression rule in GuardDuty to filter findings by automatically archiving new findings that match the specified criteria.
E. Create an AWS Lambda function that has the appropriate permissions to de-lete the finding whenever a new occurrence is reported.

Answer: C

Explanation:
"When you create an Amazon GuardDuty filter, you choose specific filter criteria, name the filter and can enable the auto-archiving of findings that the filter matches. This allows you to further tune GuardDuty to your unique environment, without degrading the ability to identify threats. With auto-archive set, all findings are still generated by GuardDuty, so you have a complete and immutable history of all suspicious activity."

NEW QUESTION 91
A company has thousands of AWS Lambda functions. While reviewing the Lambda functions, a security engineer discovers that sensitive information is being stored in environment variables and is viewable as plaintext in the Lambda console. The values of the sensitive information are only a few characters long.
What is the MOST cost-effective way to address this security issue?

A. Set up IAM policies from the Lambda console to hide access to the environment variables.
B. Use AWS Step Functions to store the environment variable
C. Access the environment variables at runtim
D. Use IAM permissions to restrict access to the environment variables to only the Lambda functions that require access.
E. Store the environment variables in AWS Secrets Manager, and access them at runtim
F. Use IAM permissions to restrict access to the secrets to only the Lambda functions that require access.
G. Store the environment variables in AWS Systems Manager Parameter Store as secure string parameters, and access them at runtim
H. Use IAM permissions to restrict access to the parameters to only the Lambda functions that require access.

Answer: D

Explanation:
Storing sensitive information in environment variables is not a secure practice, as anyone who has access to the Lambda console or the Lambda function code can view them as plaintext. To address this security issue, the security engineer needs to use a service that can store and encrypt the environment variables, and access them at runtime using IAM permissions. The most cost-effective way to do this is to use AWS Systems Manager Parameter Store, which is a service that provides secure, hierarchical storage for configuration data management and secrets management. Parameter Store allows you to store values as standard parameters (plaintext) or secure string parameters (encrypted). Secure string parameters use a AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the parameter value. To access the parameter value at runtime, the Lambda function needs to have IAM permissions to decrypt the parameter using the KMS CMK.
The other options are incorrect because:
- Option A is incorrect because setting up IAM policies from the Lambda console to hide access to the environment variables will not prevent someone who has access to the Lambda function code from viewing them as plaintext. IAM policies can only control who can perform actions on AWS resources, not what they can see in the code or the console.
- Option B is incorrect because using AWS Step Functions to store the environment variables is not a secure or cost-effective solution. AWS Step Functions is a service that lets you coordinate multiple AWS services into serverless workflows. Step Functions does not provide any encryption or secrets management capabilities, and it will incur additional charges for each state transition in the workflow. Moreover, storing environment variables in Step Functions will make them visible in the execution history of the workflow, which can be accessed by anyone who has permission to view the Step Functions console or API.
- Option C is incorrect because storing the environment variables in AWS Secrets Manager and accessing them at runtime is not a cost-effective solution. AWS Secrets Manager is a service that helps you protect secrets needed to access your applications, services, and IT resources. Secrets Manager enables you to rotate, manage, and retrieve secrets throughout their lifecycle. While Secrets Manager can securely store and encrypt environment variables using KMS CMKs, it will incur higher charges than Parameter Store for storing and retrieving secrets. Unless the security engineer needs the advanced features of Secrets Manager, such as automatic rotation of secrets or integration with other AWS services, Parameter Store is a cheaper and simpler option.

NEW QUESTION 96
A company uses Amazon API Gateway to present REST APIs to users. An API developer wants to analyze API access patterns without the need to parse the log files.
Which combination of steps will meet these requirements with the LEAST effort? (Select TWO.)

A. Configure access logging for the required API stage.
B. Configure an AWS CloudTrail trail destination for API Gateway event
C. Configure filters on the userIdentity, userAgent, and sourceIPAddress fields.
D. Configure an Amazon S3 destination for API Gateway log
E. Run Amazon Athena queries to analyze API access information.
F. Use Amazon CloudWatch Logs Insights to analyze API access information.
G. Select the Enable Detailed CloudWatch Metrics option on the required API stage.

Answer: CD

NEW QUESTION 98
A company has launched an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume in the us-east-1 Region The volume is encrypted with an AWS Key Management Service (AWS KMS) customer managed key that the company's security team created The security team has created an 1AM key policy and has assigned the policy to the key The security team has also created an 1AM instance profile and has assigned the profile to the instance
The EC2 instance will not start and transitions from the pending state to the shutting-down state to the terminated state
Which combination of steps should a security engineer take to troubleshoot this issue? (Select TWO)

A. Verify that the KMS key policy specifies a deny statement that prevents access to the key by using the aws SourceIP condition key Check that the range includes the EC2 instance IP address that is associated with the EBS volume
B. Verify that the KMS key that is associated with the EBS volume is set to the Symmetric key type
C. Verify that the KMS key that is associated with the EBS volume is in the Enabled state
D. Verify that the EC2 role that is associated with the instance profile has the correct 1AM instance policy to launch an EC2 instance with the EBS volume
E. Verify that the key that is associated with the EBS volume has not expired and needs to be rotated

Answer: CD

Explanation:
To troubleshoot the issue of an EC2 instance failing to start and transitioning to a terminated state when it has an EBS volume encrypted with an AWS KMS customer managed key, a security engineer should take the following steps:
* C. Verify that the KMS key that is associated with the EBS volume is in the Enabled state. If the key is not enabled, it will not function properly and could cause the EC2 instance to fail.
* D. Verify that the EC2 role that is associated with the instance profile has the correct IAM instance policy to launch an EC2 instance with the EBS volume. If the instance does not have the necessary permissions, it may not be able to mount the volume and could cause the instance to fail.
Therefore, options C and D are the correct answers.

NEW QUESTION 102
A company maintains an open-source application that is hosted on a public GitHub repository. While creating a new commit to the repository, an engineer uploaded their IAM access key and secret access key. The engineer reported the mistake to a manager, and the manager immediately disabled the access key. The company needs to assess the impact of the exposed access key. A security engineer must recommend a solution that requires the least possible managerial overhead.
Which solution meets these requirements?

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

Answer: A

Explanation:
To assess the impact of the exposed access key, the security engineer should recommend the following solution:
> Analyze an IAM use report from AWS Trusted Advisor to see when the access key was last used. This allows the security engineer to use a tool that provides information about IAM entities and credentials in their account, and check if there was any unauthorized activity with the exposed access key.

NEW QUESTION 105
A company's IAM account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level? Please select:

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

Answer: B

Explanation:
Option A is incorrect since you don't add a user to the IAM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach
An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group
For more information on IAM Groups, just browse to the below URL: https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
Submit your Feedback/Queries to our Experts

NEW QUESTION 106
A company is using AWS WAF to protect a customized public API service that is based on Amazon EC2 instances. The API uses an Application Load Balancer. The AWS WAF web ACL is configured with an AWS Managed Rules rule group. After a software upgrade to the API and the client application, some types of requests are no longer working and are causing application stability issues. A security engineer discovers that AWS WAF logging is not turned on for the web ACL. The security engineer needs to immediately return the application to service, resolve the issue, and ensure that logging is not turned off in the future. The security engineer turns on logging for the web ACL and specifies Amazon Cloud-Watch Logs as the destination.
Which additional set of steps should the security engineer take to meet the re-quirements?

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

Answer: A

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

NEW QUESTION 107
A company’s security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.
Which solution will meet these requirements with the LEAST amount of effort?

A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hour
B. Select theaccess-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 day
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with an event pattern that matches the compliance type of NON_COMPLIANT from AWS Config for the managed rul

D. Configure EventBridge (CloudWatch Events) to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
E. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation.Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucke
F. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucke
G. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
H. Create a script to download the IAM credentials report on a periodic basi
I. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge (Amazon CloudWatch Events). Configure the Lambda script to load the report into memory and to filter the report for recordsin which the key was last rotated at least 90 days ag
J. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
K. Create an AWS Lambda function that queries the IAM API to list all the user
L. Iterate through the users by using the ListAccessKeys operatio
M. Verify that the value in the CreateDate field is not at least 90 days ol
N. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days ol
O. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule the Lambda function to run each day.

Answer: A

NEW QUESTION 110
A developer 15 building a serverless application hosted on IAM that uses Amazon Redshift in a data store. The application has separate modules for read/write and read-only functionality. The modules need their own database users tor 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 read/write.
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 poky for each module Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call
D. Create focal 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: CD

Explanation:
To grant appropriate access to the application modules, the security engineer should do the following:
- Configure an IAM policy for each module. Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call. This allows the application modules to use temporary credentials to access the database with the permissions of the specified user.
- Create local database users for each module. This allows the security engineer to create separate users for read/write and read-only functionality, and to assign them different privileges on the database tables.

NEW QUESTION 111
You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?
Please select:

A. Add an IAM managed policy for the user
B. Add a service policy for the user
C. Add an IAM role for the user
D. Add an inline policy for the user

Answer: D

Explanation:
Options A and B are incorrect since you need to add an inline policy just for the user Option C is invalid because you don't assign an IAM role to a user
The IAM Documentation mentions the following
An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.
For more information on IAM Access and Inline policies, just browse to the below URL: https://docs.IAM.amazon.com/IAM/latest/UserGuide/access
The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

NEW QUESTION 114
A company has a guideline that mandates the encryption of all Amazon S3 bucket data in transit. A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted.
Which S3 bucket policy will meet this requirement?

A.

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

B.

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

C.

```
{
      "Version": "2012-10-17",
      "Statement": [{
                  "Sid": "AllowSSLRequestOnly",
                  "Action": "s3:*",
                  "Effect": "Deny",
                  "Resource": [
                    "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
                  ],
                  "Condition": {
                    "StringNotEquals": {
                          "s3:x-amz-server-side-encryption": "AES256"
                    }
                  },
                  "Principal": "*"
      }]
}
```

D. A screenshot of a computer code Description automatically generated

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

Answer: B

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

NEW QUESTION 117
A business stores website images in an Amazon S3 bucket. The firm serves the photos to end users through Amazon CloudFront. The firm learned lately that the photographs are being accessible from nations in which it does not have a distribution license.
Which steps should the business take to safeguard the photographs and restrict their distribution? (Select two.)

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

Answer: AC

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

NEW QUESTION 122
A company's security engineer is designing an isolation procedure for Amazon EC2 instances as part of an incident response plan. The security engineer needs to isolate a target instance to block any traffic to and from the target instance, except for traffic from the company's forensics team. Each of the company's EC2 instances has its own dedicated security group. The EC2 instances are deployed in subnets of a VPC. A subnet can contain multiple instances.
The security engineer is testing the procedure for EC2 isolation and opens an SSH session to the target instance. The procedure starts to simulate access to the target instance by an attacker. The security engineer removes the existing security group rules and adds security group rules to give the forensics team access to the target instance on port 22.
After these changes, the security engineer notices that the SSH connection is still active and usable. When the security engineer runs a ping command to the public IP address of the target instance, the ping command is blocked.
What should the security engineer do to isolate the target instance?

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

Answer: C

NEW QUESTION 125
A company became aware that one of its access keys was exposed on a code sharing website 11 days ago. A Security Engineer must review all use of the exposed access keys to determine the extent of the exposure. The company enabled IAM CloudTrail m an regions when it opened the account
Which of the following will allow (he Security Engineer 10 complete the task?

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

Answer: C

Explanation:
Amazon Athena is a service that enables you to analyze data in Amazon S3 using standard SQL1. You can use Athena to query the CloudTrail logs that are stored in S3 and filter them by the exposed access key and the date range2. The other options are not effective ways to review the use of the exposed access key.

NEW QUESTION 130
A security engineer needs to implement a solution to create and control the keys that a company uses for cryptographic operations. The security engineer must create symmetric keys in which the key material is generated and used within a custom key store that is backed by an AWS CloudHSM cluster.
The security engineer will use symmetric and asymmetric data key pairs for local use within applications. The security engineer also must audit the use of the keys.
How can the security engineer meet these requirements?

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

Answer: D

Explanation:
AWS KMS supports asymmetric KMS keys that represent a mathematically related RSA, elliptic curve (ECC), or SM2 (China Regions only) public and private key pair. These key pairs are generated in AWS KMS hardware security modules certified under the FIPS 140-2 Cryptographic Module Validation Program, except in the China (Beijing) and China (Ningxia) Regions. The private key never leaves the AWS KMS HSMs unencrypted.
https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html

NEW QUESTION 132
A company has deployed Amazon GuardDuty and now wants to implement automation for potential threats. The company has decided to start with RDP brute force attacks that come from Amazon EC2 instances in the company's AWS environment. A security engineer needs to implement a solution that blocks the detected communication from a suspicious instance until investigation and potential remediation can occur.
Which solution will meet these requirements?

A. Configure GuardDuty to send the event to an Amazon Kinesis data strea
B. Process the event with an Amazon Kinesis Data Analytics for Apache Flink application that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS). Add rules to the network ACL to block traffic to and from the suspicious instance.
C. Configure GuardDuty to send the event to Amazon EventBridge (Amazon CloudWatch Events). Deploy an AWS WAF web AC
D. Process the event with an AWS Lambda function that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS) and adds a web ACL rule to block traffic to and from the suspicious instance.
E. Enable AWS Security Hub to ingest GuardDuty findings and send the event to Amazon EventBridge (Amazon CloudWatch Events). Deploy AWS Network Firewal
F. Process the event with an AWS Lambda function that adds a rule to a Network Firewall firewall policy to block traffic to and from the suspicious instance.
G. Enable AWS Security Hub to ingest GuardDuty finding
H. Configure an Amazon Kinesis data stream as an event destination for Security Hu
I. Process the event with an AWS Lambda function that replaces the security group of the suspicious instance with a security group that does not allow any connections.

Answer: C

Explanation:
https://aws.amazon.com/blogs/security/automatically-block-suspicious-traffic-with-aws-network-firewall-and-a

NEW QUESTION 133
A company is operating a website using Amazon CloudFornt. CloudFront servers some content from Amazon S3 and other from web servers running EC2 instances behind an Application. Load Balancer (ALB). Amazon DynamoDB is used as the data store. The company already uses IAM Certificate Manager (ACM) to store a public TLS certificate that can optionally secure connections between the website users and CloudFront. The company has a new requirement to enforce end-to-end encryption in transit.
Which combination of steps should the company take to meet this requirement? (Select THREE.)

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

Answer: BCE

Explanation:
To enforce end-to-end encryption in transit, the company should do the following:
- Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB. This ensures that the data is encrypted when it travels from the web servers to the data store.
- Update the CloudFront distribution to redirect HTTP requests to HTTPS. This ensures that the viewers always use HTTPS when they access the website through CloudFront.
- Update the ALB to listen using HTTPS using the public ACM TLS certificate. Update the CloudFront distribution to connect to the HTTPS listener. This ensures that the data is encrypted when it travels from CloudFront to the ALB and from the ALB to the web servers.

NEW QUESTION 138
A company is developing an ecommerce application. The application uses Amazon EC2 instances and an Amazon RDS MySQL database. For compliance reasons, data must be secured in transit and at rest. The company needs a solution that minimizes operational overhead and minimizes cost.
Which solution meets these requirements?

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

Answer: A

NEW QUESTION 142

A company wants to configure DNS Security Extensions (DNSSEC) for the company's primary domain. The company registers the domain with Amazon Route 53. The company hosts the domain on Amazon EC2 instances by using BIND.
What is the MOST operationally efficient solution that meets this requirement?

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

Answer: D

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

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

NEW QUESTION 144
A company is hosting multiple applications within a single VPC in its IAM account. The applications are running behind an Application Load Balancer that is associated with an IAM WAF web ACL. The company's security team has identified that multiple port scans are originating from a specific range of IP addresses on the internet.
A security engineer needs to deny access from the offending IP addresses. Which solution will meet these requirements?

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

Answer: A

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

NEW QUESTION 148
A company uses a third-party application to store encrypted data in Amazon S3. The company uses another third-party application trial decrypts the data from Amazon S3 to ensure separation of duties Between the applications A Security Engineer warns to separate the permissions using IAM roles attached to Amazon EC2 instances. The company prefers to use native IAM services.
Which encryption method will meet these requirements?

A. Use encrypted Amazon EBS volumes with Amazon default keys (IAM EBS)
B. Use server-side encryption with customer-provided keys (SSE-C)
C. Use server-side encryption with IAM KMS managed keys (SSE-KMS)
D. Use server-side encryption with Amazon S3 managed keys (SSE-S3)

Answer: C

NEW QUESTION 152
A company is developing a highly resilient application to be hosted on multiple Amazon EC2 instances . The application will store highly sensitive user data in Amazon RDS tables
The application must
• Include migration to a different IAM Region in the application disaster recovery plan.
• Provide a full audit trail of encryption key administration events
• Allow only company administrators to administer keys.
• Protect data at rest using application layer encryption
A Security Engineer is evaluating options for encryption key management
Why should the Security Engineer choose IAM CloudHSM over IAM KMS for encryption key management in this situation?

A. The key administration event logging generated by CloudHSM is significantly more extensive than IAM KMS.
B. CloudHSM ensures that only company support staff can administer encryption keys, whereas IAM KMS allows IAM staff to administer keys
C. The ciphertext produced by CloudHSM provides more robust protection against brute force decryption attacks than the ciphertext produced by IAM KMS
D. CloudHSM provides the ability to copy keys to a different Region, whereas IAM KMS does not

Answer: B

Explanation:

CloudHSM allows full control of your keys such including Symmetric (AES), Asymmetric (RSA), Sha-256, SHA 512, Hash Based, Digital Signatures (RSA). On the other hand, AWS Key Management Service is a
multi-tenant key storage that is owned and managed by AWS1.
References: 1: What are the differences between AWS Cloud HSM and KMS?

NEW QUESTION 155
A Development team has built an experimental environment to test a simple stale web application It has built an isolated VPC with a private and a public subnet. The public subnet holds only an Application Load Balancer a NAT gateway, and an internet gateway. The private subnet holds ail of the Amazon EC2 instances There are 3 different types of servers Each server type has its own Security Group that limits access lo only required connectivity. The Security Groups nave both inbound and outbound rules applied Each subnet has both inbound and outbound network ACls applied to limit access to only required connectivity
Which of the following should the team check if a server cannot establish an outbound connection to the
internet? (Select THREE.)

A. The route tables and the outbound rules on the appropriate private subnet security group
B. The outbound network ACL rules on the private subnet and the Inbound network ACL rules on the public subnet
C. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet
D. The rules on any host-based firewall that may be applied on the Amazon EC2 instances
E. The Security Group applied to the Application Load Balancer and NAT gateway
F. That the 0.0.0./0 route in the private subnet route table points to the internet gateway in the public subnet

Answer: CEF

Explanation:
because these are the factors that could affect the outbound connection to the internet from a server in a private subnet. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet must allow the traffic to pass through8. The security group applied to the application load balancer and NAT gateway must also allow the traffic from the private subnet9. The 0.0.0.0/0 route in the private subnet route table must point to the NAT gateway in the public subnet, not the internet gateway10. The other options are either irrelevant or incorrect for troubleshooting the outbound connection issue.

NEW QUESTION 160
A company's Security Engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other AWS services. The contractor's IAM account must not be able to gain access to any other AWS service, even if the IAM account is assigned additional permissions based on IAM group membership.
What should the Security Engineer do to meet these requirements?

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

Answer: B

NEW QUESTION 164
Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?
Please select:

A. Use the application to rotate the keys in every 2 months via the SDK
B. Use a script to query the creation date of the key
C. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.
D. Delete the user associated with the keys after every 2 month
E. Then recreate the user again.
F. Delete the IAM Role associated with the keys after every 2 month
G. Then recreate the IAM Role again.

Answer: B

Explanation:
One can use the CLI command list-access-keys to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted.
The Returns list-access-keys CLI command returns information about the access key IDs associated with the specified IAM user. If there are none, the action returns an empty list
Option A is incorrect because you might as use a script for such maintenance activities Option C is incorrect because you would not rotate the users themselves Option D is incorrect because you don't use IAM roles for such a purpose For more information on the CLI command, please refer to the below Link:
http://docs.IAM.amazon.com/cli/latest/reference/iam/list-access-keys.htmll
The correct answer is: Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.
Submit your Feedback/Queries to our Experts

NEW QUESTION 168
A company wants to receive an email notification about critical findings in AWS Security Hub. The company does not have an existing architecture that supports this functionality.
Which solution will meet the requirement?

A. Create an AWS Lambda function to identify critical Security Hub finding
B. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the Lambda functio
C. Subscribe an email endpoint to the SNS topic to receive published messages.

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

Answer: C

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

NEW QUESTION 171
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your AWS-Certified-Security-Specialty Exam with Our Prep Materials Via below:

https://www.certleader.com/AWS-Certified-Security-Specialty-dumps.html