Exam Questions SCS-C02

AWS Certified Security - Specialty

https://www.2passeasy.com/dumps/SCS-C02/

NEW QUESTION 1
An AWS account that is used for development projects has a VPC that contains two subnets. The first subnet is named public-subnet-1 and has the CIDR block 192.168.1.0/24 assigned. The other subnet is named private-subnet-2 and has the CIDR block 192.168.2.0/24 assigned. Each subnet contains Amazon EC2 instances.
Each subnet is currently using the VPC's default network ACL. The security groups that the EC2 instances in these subnets use have rules that allow traffic between each instance where required. Currently, all network traffic flow is working as expected between the EC2 instances that are using these subnets.
A security engineer creates a new network ACL that is named subnet-2-NACL with default entries. The security engineer immediately configures private-subnet-2 to use the new network ACL and makes no other changes to the infrastructure. The security engineer starts to receive reports that the EC2 instances in public-subnet-1 and public-subnet-2 cannot communicate with each other.
Which combination of steps should the security engineer take to allow the EC2 instances that are running in these two subnets to communicate again? (Select TWO.)

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

Answer: CE

Explanation:
The AWS documentation states that you can add an outbound allow rule for 192.168.2.0/24 in
subnet-2-NACL and add an outbound allow rule for 192.168.1.0/24 in subnet-2-NACL. This will allow the EC2 instances that are running in these two subnets to communicate again.
References: : Amazon VPC User Guide

NEW QUESTION 2
A company in France uses Amazon Cognito with the Cognito Hosted UI as an identity broker for sign-in and sign-up processes. The company is marketing an application and expects that all the application's users will come from France.
When the company launches the application the company's security team observes fraudulent sign-ups for the application. Most of the fraudulent registrations are from users outside of France.
The security team needs a solution to perform custom validation at sign-up Based on the results of the validation the solution must accept or deny the registration request.
Which combination of steps will meet these requirements? (Select TWO.)

A. Create a pre sign-up AWS Lambda 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 UI.
G. Update the application's Amazon Cognito user pool to configure a geographic restriction setting.
H. Use Amazon Cognito to configure a social identity provider (IdP) to validate the requests on the hosted UI.

Answer: B

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

NEW QUESTION 3
A company stores sensitive documents in Amazon S3 by using server-side encryption with an IAM Key Management Service (IAM KMS) CMK. A new requirement mandates that the CMK that is used for these documents can be used only for S3 actions.
Which statement should the company add to the key policy to meet this requirement?
A)

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

B)

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

A. Option A
B. Option B

Answer: A

NEW QUESTION 4
A company's security team is building a solution for logging and visualization. The solution will assist the company with the large variety and velocity of data that it receives from IAM across multiple accounts. The security team has enabled IAM CloudTrail and VPC Flow Logs in all of its accounts. In addition, the company has an organization in IAM Organizations and has an IAM Security Hub master account.
The security team wants to use Amazon Detective However the security team cannot enable Detective and is unsure why
What must the security team do to enable Detective?

A. Enable Amazon Macie so that Secunty H jb will allow Detective to process findings from Macie.
B. Disable IAM Key Management Service (IAM KMS) encryption on CtoudTrail logs in every member account of the organization
C. Enable Amazon GuardDuty on all member accounts Try to enable Detective in 48 hours
D. Ensure that the principal that launches Detective has the organizations ListAccounts permission

Answer: D

NEW QUESTION 5
A company hosts an end user application on AWS Currently the company deploys the application on Amazon EC2 instances behind an Elastic Load Balancer The company wants to configure end-to-end encryption between the Elastic Load Balancer and the EC2 instances.
Which solution will meet this requirement with the LEAST operational effort?

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

Answer: A

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

NEW QUESTION 6
Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement.
Please select:

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

Answer: A

Explanation:
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another IAM account within a single region.
Options B and C are invalid because you need to use VPC Peering Option D is invalid because VPC Peering is available
For more information on VPC Peering please see the below Link:
http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html
The correct answer is: Set up VPC peering between the central server VPC and each of the teams VPCs. Submit your Feedback/Queries to our Experts

NEW QUESTION 7
A company hosts a public website on an Amazon EC2 instance. HTTPS traffic must be able to access the website. The company uses SSH for management of the web server.
The website is on the subnet 10.0.1.0/24. The management subnet is 192.168.100.0/24. A security engineer must create a security group for the EC2 instance.

Which combination of steps should the security engineer take to meet these requirements in the MOST secure manner? (Select TWO.)

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

Answer: BC

Explanation:
The correct answer is B and C.
* B. Allow port 443 from source 0.0.0.0/0.
This is correct because port 443 is used for HTTPS traffic, which must be able to access the website from any source IP address.
* C. Allow port 22 from 192.168.100.0/24.
This is correct because port 22 is used for SSH, which is the management protocol for the web server. The management subnet is 192.168.100.0/24, so only this subnet should be allowed to access port 22.
* A. Allow port 22 from source 0.0.0.0/0.
This is incorrect because it would allow anyone to access port 22, which is a security risk. SSH should be restricted to the management subnet only.
* D. Allow port 22 from 10.0.1.0/24.
This is incorrect because it would allow the website subnet to access port 22, which is unnecessary and a security risk. SSH should be restricted to the management subnet only.
* E. Allow port 443 from 10.0.1.0/24.
This is incorrect because it would limit the HTTPS traffic to the website subnet only, which defeats the purpose of having a public website.

NEW QUESTION 8
A company has developed a new Amazon RDS database application. The company must secure the ROS database credentials for encryption in transit and encryption at rest. The company also must rotate the credentials automatically on a regular basis.
Which solution meets these requirements?

A. Use IAM Systems Manager Parameter Store to store the database credentiai
B. Configure automatic rotation of the credentials.
C. Use IAM Secrets Manager to store the database credential
D. Configure automat* rotation of the credentials
E. Store the database credentials in an Amazon S3 bucket that is configured with server-side encryption with S3 managed encryption keys (SSE-S3) Rotate the credentials with IAM database authentication.
F. Store the database credentials m Amazon S3 Glacier, and use S3 Glacier Vault Lock Configure an IAM Lambda function to rotate the credentials on a scheduled basts

Answer: A

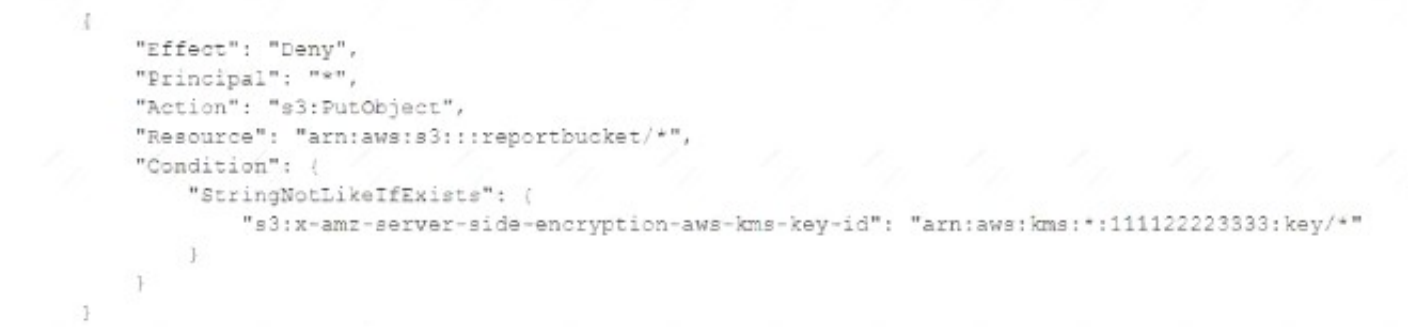
NEW QUESTION 9
A company uses an Amazon S3 bucket to store reports Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client-specified IAM Key Management Service (IAM KMS) CMK owned by the same account as the S3 bucket. The 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.



E. Option A
F. Option B
G. Option C
H. Option D

Answer: D

NEW QUESTION 10
A company plans to use AWS Key Management Service (AWS KMS) to implement an encryption strategy to protect data at rest. The company requires client-side encryption for company projects. The company is currently conducting multiple projects to test the company's use of AWS KMS. These tests have led to a sudden increase in the company's AWS resource consumption. The test projects include applications that issue multiple requests each second to KMS endpoints for encryption activities.
The company needs to develop a solution that does not throttle the company's ability to use AWS KMS. The solution must improve key usage for client-side encryption and must be cost optimized. Which solution will meet these requirements?

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

Answer: B

Explanation:
The correct answer is B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.
This answer is correct because data key caching can improve performance, reduce cost, and help the company stay within the service limits of AWS KMS. Data key caching stores data keys and related cryptographic material in a cache, and reuses them for encryption and decryption operations. This reduces the number of requests to AWS KMS endpoints and avoids throttling. The AWS Encryption SDK provides a local cache and a caching cryptographic materials manager (caching CMM) that interacts with the cache and enforces security thresholds that the company can set1.
The other options are incorrect because:

- A. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization. Keyrings are used to generate, encrypt, and decrypt data keys, but they do not cache or reuse them. Using each keyring individually or combining them into a multi-keyring does not reduce the number of requests to AWS KMS endpoints2.
- C. Using KMS key rotation does not address the problem of throttling or cost optimization. Key rotation is a security practice that creates new cryptographic material for a KMS key every year, but it does not affect the data that the KMS key protects. Key rotation does not reduce the number of requests to AWS KMS endpoints, and it might incur additional costs for storing multiple versions of key material3.
- D. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization, as explained in option A. Moreover, using any of the wrapping keys in the multi-keyring to decrypt the data is not a valid option, because only one of the wrapping keys can decrypt a given data key. The wrapping key that encrypts a data key is stored in the encrypted data key structure, and only that wrapping key can decrypt it4.

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

NEW QUESTION 10
A web application gives users the ability to log in verify their membership's validity and browse artifacts that are stored in an Amazon S3 bucket. When a user attempts to download an object, the application must verify the permission to access the object and allow the user to download the object from a custom domain name such as example com.
What is the MOST secure way for a security engineer to implement this functionality?

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

Answer: D

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

NEW QUESTION 13
A company has several workloads running on AWS. Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the Security Engineer implement employee-only access to this system without changing the application?

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

Answer: A

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

NEW QUESTION 14
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 15
A security team is developing an application on an Amazon EC2 instance to get objects from an Amazon S3 bucket. All objects in the S3 bucket are encrypted with an AWS Key Management Service (AWS KMS) customer managed key. All network traffic for requests that are made within the VPC is restricted to the AWS infrastructure. This traffic does not traverse the public internet.
The security team is unable to get objects from the S3 bucket Which factors could cause this issue? (Select THREE.)

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

Answer: ADE

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html
To get objects from an S3 bucket that are encrypted with a KMS customer managed key, the security team needs to have the following factors in place:

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

NEW QUESTION 18
A company is building an application on AWS that will store sensitive information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.
What should the security engineer recommend?

A. Enable Amazon RDS encryption to encrypt the database and snapshot
B. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instance
C. Include the database credential in the EC2 user data fiel
D. Use an AWS Lambda function to rotate database credential
E. Set up TLS for the connection to the database.

F. Install a database on an Amazon EC2 instanc
G. Enable third-party disk encryption to encrypt Amazon Elastic Block Store (Amazon EBS) volum
H. Store the database credentials in AWS 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 AWS Secrets Manager with automatic rotatio
M. Set up TLS for the connection to the RDS hosted database.
N. Set up an AWS CloudHSM cluster with AWS Key Management Service (AWS KMS) to store KMS key
O. Set up Amazon RDS encryption using AWS KSM to encrypt the databas
P. Store the database credentials in AWS Systems Manager Parameter Store with automatic rotatio
Q. Set up TLS for the connection to the RDS hosted database.

Answer: C

NEW QUESTION 21
A company hosts business-critical applications on Amazon EC2 instances in a VPC. The VPC uses default DHCP options sets. A security engineer needs to log all DNS queries that internal resources make in the VPC. The security engineer also must create a list of the most common DNS queries over time.
Which solution will meet these requirements?

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

Answer: D

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

NEW QUESTION 25
A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company's security policies for accessing other AWS resources from Amazon EC2.
A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLE-BUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.
The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).
Which combination of steps should the security engineer take to gather this information? (Choose two.)

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

Answer: AD

NEW QUESTION 29
A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.
The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.
Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

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

Answer: BCF

NEW QUESTION 31

Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

A. Default AWS Certificate Manager certificate
B. Custom SSL certificate stored in AWS KMS
C. Default CloudFront certificate
D. Custom SSL certificate stored in AWS Certificate Manager
E. Default SSL certificate stored in AWS Secrets Manager
F. Custom SSL certificate stored in AWS IAM

Answer: ABC

Explanation:
The key length for an RSA certificate that you use with CloudFront is 2048 bits, even though ACM supports larger keys. If you use an imported certificate with CloudFront, your key length must be 1024 or 2048 bits and cannot exceed 2048 bits. You must import the certificate in the US East (N. Virginia) Region. You must have permission to use and import the SSL/TLS certificate
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

NEW QUESTION 36
A company wants to monitor the deletion of AWS Key Management Service (AWS KMS) customer managed keys. A security engineer needs to create an alarm that will notify the company before a KMS key is deleted. The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch.
What should the security engineer do next to meet these requirements?

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

Answer: C

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

NEW QUESTION 40
A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot. What should the Security Engineer do to block the malicious bot?

A. Add a deny rule to the public VPC security group to block the malicious IP
B. Add the malicious IP to IAM WAF backhsted IPs
C. Configure Linux iptables or Windows Firewall to block any traffic from the malicious IP
D. Modify the hosted zone in Amazon Route 53 and create a DNS sinkhole for the malicious IP

Answer: D

Explanation:
what the Security Engineer should do to block the malicious bot. SFTP is a protocol that allows secure file transfer over SSH. EC2 is a service that provides virtual servers in the cloud. A public subnet is a subnet that has a route to an internet gateway, which allows it to communicate with the internet. A brute force attack is a type of attack that tries to guess passwords or keys by trying many possible combinations. A malicious bot is a software program that performs automated tasks for malicious purposes. Route 53 is a service that provides DNS resolution and domain name registration. A DNS sinkhole is a technique that redirects malicious or unwanted traffic to a different destination, such as a black hole server or a honeypot. By modifying the hosted zone in Route 53 and creating a DNS sinkhole for the malicious IP, the Security Engineer can block the malicious bot from reaching the EC2 instance on the public subnet. The other options are either ineffective or inappropriate for blocking the malicious bot.

NEW QUESTION 42
Your company is planning on using bastion hosts for administering the servers in IAM. Which of the following is the best description of a bastion host from a security perspective?
Please select:

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

Answer: C

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

In IAM, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.
Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring For more information on bastion hosts, just browse to the below URL:
https://docsIAM.amazon.com/quickstart/latest/linux-bastion/architecture.htl
The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.
Submit your Feedback/Queries to our Experts

NEW QUESTION 47
A Network Load Balancer (NLB) target instance is not entering the InService state. A security engineer determines that health checks are failing.
Which factors could cause the health check failures? (Select THREE.)

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

Answer: ACD

NEW QUESTION 48
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 53
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 56
Your CTO thinks your IAM account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated IAM engineers and doing everything they can to cover their tracks?
Please select:

A. Use CloudTrail Log File Integrity Validation.
B. Use IAM Config SNS Subscriptions and process events in real time.
C. Use CloudTrail backed up to IAM S3 and Glacier.
D. Use IAM Config Timeline forensics.

Answer: A

Explanation:
The IAM Documentation mentions the following
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. You can use the IAM CLI to validate the files in the location where CloudTrail delivered them
Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs For more information on Cloudtrail log file validation, please visit the below URL: http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html
The correct answer is: Use CloudTrail Log File Integrity Validation. omit your Feedback/Queries to our Expert

NEW QUESTION 59
A company uses AWS Organizations and has production workloads across multiple AWS accounts. A security engineer needs to design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads.
The solution must automate remediation of incidents across the production accounts. The solution also must publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic when a critical security finding is detected. In addition, the solution must send all security incident logs to a dedicated account.
Which solution will meet these requirements?

A. Activate Amazon GuardDuty in each production accoun
B. In a dedicated logging accoun
C. aggregate all GuardDuty logs from each production accoun
D. Remediate incidents by configuring GuardDuty to directly invoke an AWS Lambda functio
E. Configure the Lambda function to also publish notifications to the SNS topic.
F. Activate AWS security Hub in each production accoun
G. In a dedicated logging accoun
H. aggregate all security Hub findings from each production accoun
I. Remediate incidents by ustng AWS Config and AWS Systems Manage
J. Configure Systems Manager to also pub11Sh notifications to the SNS topic.
K. Activate Amazon GuardDuty in each production accoun
L. In a dedicated logging accoun
M. aggregate all GuardDuty logs from each production account Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the GuardDuty finding
N. Configure the Lambda function to also publish notifications to the SNS topic.
O. Activate AWS Security Hub in each production accoun
P. In a dedicated logging accoun
Q. aggregate all Security Hub findings from each production accoun
R. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the Security Hub finding
S. Configure the Lambda function to also publish notifications to the SNS topic.

Answer: D

Explanation:
The correct answer is D.
To design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads, the security engineer needs to use a service that can aggregate and analyze security findings from multiple sources. AWS Security Hub is a service that provides a comprehensive view of your security posture across your AWS accounts and enables you to check your environment against security standards and best practices. Security Hub also integrates with other AWS services, such as Amazon GuardDuty, AWS Config, and AWS Systems Manager, to collect and correlate security findings.
To automate remediation of incidents across the production accounts, the security engineer needs to use a service that can trigger actions based on events. Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from a variety of sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke a custom AWS Lambda function from the Security Hub findings. Lambda is a serverless compute service that lets you run code without provisioning or managing servers.
To publish a notification to an Amazon SNS topic when a critical security finding is detected, the security engineer needs to use a service that can send messages to subscribers. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can configure the Lambda function to also publish notifications to the SNS topic.
To send all security incident logs to a dedicated account, the security engineer needs to use a service that can aggregate and store log data from multiple sources. AWS Security Hub allows you to aggregate security findings from multiple accounts into a single account using the delegated administrator feature. This feature enables you to designate an AWS account as the administrator for Security Hub in an organization. The administrator account can then view and manage Security Hub findings from all member accounts.
Therefore, option D is correct because it meets all the requirements of the solution. Option A is incorrect because GuardDuty does not provide a comprehensive view of your security posture across your AWS accounts. GuardDuty is primarily a threat detection service that monitors for malicious or unauthorized behavior. Option B is incorrect because Config and Systems Manager are not designed to automate remediation of incidents based on Security Hub findings. Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources, while Systems Manager is a service that allows you to manage your infrastructure on AWS at scale. Option C is incorrect because GuardDuty does not provide a comprehensive view of your security posture across your AWS accounts.
References:

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

NEW QUESTION 63
Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets.
Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC. These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table.
The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.
How will the security engineer be able to comply with these requirements?

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

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

Answer: C

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

NEW QUESTION 64
A Security Engineer is troubleshooting an issue with a company's custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events lo an Amazon SNS topic. All logs are encrypted at rest using an IAM KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.
The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No togs are being received.
What should the Security Engineer do to troubleshoot this issue?
A) Add the following statement to the IAM managed CMKs:

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

B)
Add the following statement to the CMK key policy:

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

C)
Add the following statement to the CMK key policy:

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

D)
Add the following statement to the CMK key policy:

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

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

Answer: D

NEW QUESTION 69
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 71
A company is running an application in The eu-west-1 Region. The application uses an IAM Key Management Service (IAM KMS) CMK to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region.
A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code.
Which change should the security engineer make to the IAM KMS configuration to meet these requirements?

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

Answer: B

NEW QUESTION 72
A company needs a security engineer to implement a scalable solution for multi-account authentication and authorization. The solution should not introduce additional user-managed architectural components. Native IAM features should be used as much as possible The security engineer has set up IAM Organizations w1th all features activated and IAM SSO enabled.
Which additional steps should the security engineer take to complete the task?

A. Use AD Connector to create users and groups for all employees that require access to IAM accounts.Assign AD Connector groups to IAM accounts and link to the IAM roles in accordance with the employees‘job functions and access requirements Instruct employees to access IAM accounts by using the IAM Directory Service user portal.
B. Use an IAM SSO default directory to create users and groups for all employees that require access to IAM account
C. Assign groups to IAM accounts and link to permission sets in accordance with the employees‘job functions and access requirement
D. Instruct employees to access IAM accounts by using the IAM SSO user portal.
E. Use an IAM SSO default directory to create users and groups for all employees that require access to IAM account
F. Link IAM SSO groups to the IAM users present in all accounts to inherit existing permission
G. Instruct employees to access IAM accounts by using the IAM SSO user portal.
H. Use IAM Directory Service tor Microsoft Active Directory to create users and groups for all employees that require access to IAM accounts Enable IAM Management Console access in the created directory and specify IAM SSO as a source cl information tor integrated accounts and permission set
I. Instruct employees to access IAM accounts by using the IAM Directory Service user portal.

Answer: B

NEW QUESTION 73
A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM.
Which combination of IAM services and features will provide protection in this scenario? (Select THREE).

A. Amazon Route 53
B. IAM Certificate Manager (ACM)
C. Amazon S3
D. IAM Shield
E. Elastic Load Balancer
F. Amazon GuardDuty

Answer: DEF

NEW QUESTION 78
A company's security engineer is developing an incident response plan to detect suspicious activity in an AWS account for VPC hosted resources. The security engineer needs to provide visibility for as many AWS Regions as possible.
Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)

A. Turn on VPC Flow Logs for all VPCs in the account.
B. Activate Amazon GuardDuty across all AWS Regions.
C. Activate Amazon Detective across all AWS Regions.
D. Create an Amazon Simple Notification Service (Amazon SNS) topi
E. Create an Amazon EventBridge rule that responds to findings and publishes the find-ings to the SNS topic.
F. Create an AWS Lambda functio
G. Create an Amazon EventBridge rule that in-vokes the Lambda function to publish findings to Amazon Simple Email Ser-vice (Amazon SES).

Answer: BD

Explanation:
To detect suspicious activity in an AWS account for VPC hosted resources, the security engineer needs to use a service that can monitor network traffic and API calls across all AWS Regions. Amazon GuardDuty is a threat detection service that can do this by analyzing VPC Flow Logs, AWS CloudTrail event logs, and DNS logs. By activating GuardDuty across all AWS Regions, the security engineer can provide visibility for as many regions as possible. GuardDuty generates findings that contain details about the potential threats detected in the account. To respond to these findings, the security engineer needs to create a mechanism that can notify the relevant stakeholders or take remedial actions. One way to do this is to use Amazon EventBridge, which is a serverless event bus service that can connect AWS services and third-party applications. By creating an EventBridge rule that responds to GuardDuty findings and publishes them to an Amazon Simple Notification Service (Amazon SNS) topic, the security engineer can enable subscribers of the topic to receive notifications via email, SMS, or other methods. This is a cost-effective solution that does not require any additional infrastructure or code.

NEW QUESTION 79
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 80
A company is using AWS Organizations to manage multiple accounts. The company needs to allow an IAM user to use a role to access resources that are in another organization's AWS account.
Which combination of steps must the company perform to meet this requirement? (Select TWO.)

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

J. Attach the identity policy to the role.

Answer: BC

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

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

Verified References:

- https://repost.aws/knowledge-center/cross-account-access-iam
- https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html
- https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

NEW QUESTION 84
A company needs to follow security best practices to deploy resources from an AWS CloudFormation template. The CloudFormation template must be able to configure sensitive database credentials.
The company already uses AWS Key Management Service (AWS KMS) and AWS Secrets Manager. Which solution will meet the requirements?

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

Answer: A

Explanation:

- Option A: This option meets the requirements of following security best practices and configuring sensitive database credentials in the CloudFormation template. A dynamic reference is a way to specify external values that are stored and managed in other services, such as Secrets Manager, in the stack templates1. When using a dynamic reference, CloudFormation retrieves the value of the specified reference when necessary during stack and change set operations1. Dynamic references can be used for certain resources that support them, such as AWS::RDS::DBInstance1. By using a dynamic reference to reference the database credentials in Secrets Manager, the company can leverage the existing integration between these services and avoid hardcoding the secret information in the template. Secrets Manager is a service that helps you protect secrets needed to access your applications, services, and IT resources2. Secrets Manager enables you to rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle2.

NEW QUESTION 88
A company is running an Amazon RDS for MySQL DB instance in a VPC. The VPC must not send or receive network traffic through the internet.
A security engineer wants to use AWS Secrets Manager to rotate the DB instance credentials automatically. Because of a security policy, the security engineer cannot use the standard AWS Lambda function that Secrets Manager provides to rotate the credentials.
The security engineer deploys a custom Lambda function in the VPC. The custom Lambda function will be responsible for rotating the secret in Secrets Manager.
The security engineer edits the DB instance's security group to allow connections from this function. When the function is invoked, the function cannot communicate with Secrets Manager to rotate the secret properly.
What should the security engineer do so that the function can rotate the secret?

A. Add an egress-only internet gateway to the VP
B. Allow only the Lambda function's subnet to route traffic through the egress-only internet gateway.
C. Add a NAT gateway to the VP
D. Configure only the Lambda function's subnet with a default route through the NAT gateway.
E. Configure a VPC peering connection to the default VPC for Secrets Manage
F. Configure the Lambda function's subnet to use the peering connection for routes.
G. Configure a Secrets Manager interface VPC endpoin
H. Include the Lambda function's private subnet during the configuration process.

Answer: D

Explanation:
You can establish a private connection between your VPC and Secrets Manager by creating an interface VPC endpoint. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access Secrets Manager APIs without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Reference:
https://docs.aws.amazon.com/secretsmanager/latest/userguide/vpc-endpoint-overview.html
The correct answer is D. Configure a Secrets Manager interface VPC endpoint. Include the Lambda function's private subnet during the configuration process.
A Secrets Manager interface VPC endpoint is a private connection between the VPC and Secrets Manager that does not require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection1. By configuring a Secrets Manager interface VPC endpoint, the security engineer can enable the custom Lambda function to communicate with Secrets Manager without sending or receiving network traffic through the internet. The security engineer must include the Lambda function's private subnet during the configuration process to allow the function to use the endpoint2.
The other options are incorrect for the following reasons:

- A. An egress-only internet gateway is a VPC component that allows outbound communication over IPv6 from instances in the VPC to the internet, and prevents the internet from initiating an IPv6 connection with the instances3. However, this option does not meet the requirement that the VPC must not send or receive network traffic through the internet. Moreover, an egress-only internet gateway is for use with IPv6 traffic only, and Secrets Manager does not support IPv6 addresses2.
- B. A NAT gateway is a VPC component that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections with those instances4. However, this option does not meet the requirement that the VPC must not send or receive network traffic through the internet. Additionally, a NAT gateway requires an elastic IP address, which is a public IPv4 address4.

C. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses5. However, this option does not work because Secrets Manager does not have a default VPC that can be peered with. Furthermore, a VPC peering connection does not provide a private connection to Secrets Manager APIs without an internet gateway or other devices2.

NEW QUESTION 89
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 91
A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company has set up Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers.
A new security mandate requires the company to implement a solution to log and query DNS traffic that goes to the on-premises DNS servers. The logs must show details of the source IP address of the instance from which the query originated. The logs also must show the DNS name that was requested in Route 53 Resolver.
Which solution will meet these requirements?

A. Use VPC Traffic Mirrorin
B. Configure all relevant elastic network interfaces as the traffic source, include amazon-dns in the mirror filter, and set Amazon CloudWatch Logs as the mirror targe
C. Use CloudWatch Insights on the mirror session logs to run queries on the source IP address and DNS name.
D. Configure VPC flow logs on all relevant VPC
E. Send the logs to an Amazon S3 bucke
F. Use Amazon Athena to run SQL queries on the source IP address and DNS name.
G. Configure Route 53 Resolver query logging on all relevant VPC
H. Send the logs to Amazon CloudWatch Log
I. Use CloudWatch Insights to run queries on the source IP address and DNS name.
J. Modify the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS server
K. Send the logs to an Amazon S3 bucke
L. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

Answer: C

Explanation:
The correct answer is C. Configure Route 53 Resolver query logging on all relevant VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Insights to run queries on the source IP address and DNS name.
According to the AWS documentation1, Route 53 Resolver query logging lets you log the DNS queries that Route 53 Resolver handles for your VPCs. You can send the logs to CloudWatch Logs, Amazon S3, or Kinesis Data Firehose. The logs include information such as the following:

- The AWS Region where the VPC was created
- The ID of the VPC that the query originated from
- The IP address of the instance that the query originated from
- The instance ID of the resource that the query originated from
- The date and time that the query was first made
- The DNS name requested (such as prod.example.com)
- The DNS record type (such as A or AAAA)
- The DNS response code, such as NoError or ServFail
- The DNS response data, such as the IP address that is returned in response to the DNS query

You can use CloudWatch Insights to run queries on your log data and analyze the results using graphs and statistics2. You can filter and aggregate the log data based on any field, and use operators and functions to perform calculations and transformations. For example, you can use CloudWatch Insights to find out how many queries were made for a specific domain name, or which instances made the most queries.
Therefore, this solution meets the requirements of logging and querying DNS traffic that goes to the
on-premises DNS servers, showing details of the source IP address of the instance from which the query originated, and the DNS name that was requested in Route 53 Resolver.
The other options are incorrect because:

- A. Using VPC Traffic Mirroring would not capture the DNS queries that go to the on-premises DNS servers, because Traffic Mirroring only copies network traffic from an elastic network interface of an EC2 instance to a target for analysis3. Traffic Mirroring does not include traffic that goes through a Route 53 Resolver outbound endpoint, which is used to forward queries to on-premises DNS servers4. Therefore, this solution would not meet the requirements.
- B. Configuring VPC flow logs on all relevant VPCs would not capture the DNS name that was requested in Route 53 Resolver, because flow logs only record information about the IP traffic going to and from network interfaces in a VPC5. Flow logs do not include any information about the content or payload of a packet, such as a DNS query or response. Therefore, this solution would not meet the requirements.
- D. Modifying the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS servers would not enable logging of DNS queries, because Resolver rules only specify how to forward queries for specified domain names to your network6. Resolver rules do not have any logging functionality by themselves. Therefore, this solution would not meet the requirements. References:

1: Resolver query logging - Amazon Route 53 2: Analyzing log data with CloudWatch Logs Insights - Amazon CloudWatch 3: What is Traffic Mirroring? - Amazon Virtual Private Cloud 4: Outbound Resolver endpoints - Amazon Route 53 5: Logging IP traffic using VPC Flow Logs - Amazon Virtual Private Cloud 6: Managing forwarding rules - Amazon Route 53

NEW QUESTION 92
There is a requirement for a company to transfer large amounts of data between IAM and an on-premise location. There is an additional requirement for low latency and high consistency traffic to IAM. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below
Please select:

A. Provision a Direct Connect connection to an IAM region using a Direct Connect partner.
B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.
C. Create an iPSec tunnel for private connectivity, which increases network consistency and reduces latency.
D. Create a VPC peering connection between IAM and the Customer gateway.

Answer: A

Explanation:
IAM Direct Connect makes it easy to establish a dedicated network connection from your premises to IAM. Using IAM Direct Connect you can establish private connectivity between IAM and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than Internet-based connections.
Options B and C are invalid because these options will not reduce network latency Options D is invalid because this is only used to connect 2 VPC's
For more information on IAM direct connect, just browse to the below URL: https://IAM.amazon.com/directconnect
The correct answer is: Provision a Direct Connect connection to an IAM region using a Direct Connect partner. omit your Feedback/Queries to our Experts

NEW QUESTION 97
A security engineer needs to configure an Amazon S3 bucket policy to restrict access to an S3 bucket that is named DOC-EXAMPLE-BUCKET. The policy must allow access to only DOC-EXAMPLE-BUCKET from only the following endpoint: vpce-1a2b3c4d. The policy must deny all access to DOC-EXAMPLE-BUCKET if the specified endpoint is not used.
Which bucket policy statement meets these requirements?

A. A computer code with black text Description automatically generated

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

B. A computer code with black text Description automatically generated

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

C. A computer code with black text Description automatically generated

D. A computer code with black text Description automatically generated

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

Answer: B

Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html

NEW QUESTION 102
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 105
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 109
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 114
A company is using IAM Organizations. The company wants to restrict IAM usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new IAM accounts under the development OU.

A. Include the following SCP on the development OU

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

B. Include the following SCP on the development account

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

C. Include the following SCP on the development OU

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

D. Include the following SCP on the development OU

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

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

Answer: A

NEW QUESTION 116
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 120
A company uses Amazon EC2 Linux instances in the AWS Cloud. A member of the company's security team recently received a report about common vulnerability identifiers on the instances.
A security engineer needs to verify patching and perform remediation if the instances do not have the correct patches installed. The security engineer must determine which EC2 instances are at risk and must implement a solution to automatically update those instances with the applicable patches.
What should the security engineer do to meet these requirements?

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

Answer: A

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

NEW QUESTION 124
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 128
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 133
An international company has established a new business entity in South Korea. The company also has established a new AWS account to contain the workload for the South Korean region. The company has set up the workload in the new account in the ap-northeast-2 Region. The workload consists of three Auto Scaling groups of Amazon EC2 instances. All workloads that operate in this Region must keep system logs and application logs for 7 years.
A security engineer must implement a solution to ensure that no logging data is lost for each instance during scaling activities. The solution also must keep the logs for only the required period of 7 years.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

A. Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launc
B. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs.
C. Set the log retention for desired log groups to 7 years.
D. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use.Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.
E. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use.Configure the role to provide the necessary permissions to forward logs to Amazon S3.
F. Ensure that a log forwarding application is installed on all the EC2 instances that the Auto Scaling groups launc
G. Configure the log forwarding application to periodically bundle the logs and forward the logs to Amazon S3.
H. Configure an Amazon S3 Lifecycle policy on the target S3 bucket to expire objects after 7 years.

Answer: ABC

Explanation:
The correct combination of steps that the security engineer should take to meet these requirements are A. Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launch. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs., B. Set the log retention for desired log groups to 7 years., and C. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.
* A. This answer is correct because it meets the requirement of ensuring that no logging data is lost for each instance during scaling activities. By installing the CloudWatch agent on all the EC2 instances, the security engineer can collect and send system logs and application logs to CloudWatch Logs, which is a service that stores and monitors log data. By generating a CloudWatch agent configuration file, the security engineer can specify which logs to forward and how often.
* B. This answer is correct because it meets the requirement of keeping the logs for only the required period of 7 years. By setting the log retention for desired log groups, the security engineer can control how long
CloudWatch Logs retains log events before deleting them. The security engineer can choose a predefined retention period of 7 years, or use a custom value.
* C. This answer is correct because it meets the requirement of providing the necessary permissions to forward logs to CloudWatch Logs. By attaching an IAM role to the launch configuration or launch template that the Auto Scaling groups use, the security engineer can grant permissions to the EC2 instances that are launched by the Auto Scaling groups. By configuring the role to provide the necessary permissions, such as cloudwatch:PutLogEvents and cloudwatch:CreateLogStream, the security engineer can allow the EC2 instances to send log data to CloudWatch Logs.

NEW QUESTION 137
A company is deploying an Amazon EC2-based application. The application will include a custom health-checking component that produces health status data in JSON format. A Security Engineer must
implement a secure solution to monitor application availability in near-real time by analyzing the hearth status data.
Which approach should the Security Engineer use?

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

Answer: A

Explanation:
Amazon CloudWatch monitoring is a service that collects and tracks metrics from AWS resources and applications, and provides visualization tools and alarms to monitor performance and availability1. The health status data in JSON format can be sent to CloudWatch as custom metrics2, and then displayed in CloudWatch dashboards3. The other options are either inefficient or insecure for monitoring application availability in near-real time.

NEW QUESTION 141
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 143
You have an S3 bucket defined in IAM. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this. Please select:

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

Answer: B

Explanation:
One can use the IAM Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL:
https://IAM.amazonxom/blogs/securirv/how4o-encrvpt-and-decrypt-your-data-with-the-IAM-encryption-cl The correct answer is: Use the IAM Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

NEW QUESTION 148
An organization wants to log all IAM API calls made within all of its IAM accounts, and must have a central place to analyze these logs. What steps should be taken to meet these requirements in the MOST secure manner? (Select TWO)

A. Turn on IAM CloudTrail in each IAM account
B. Turn on CloudTrail in only the account that will be storing the logs
C. Update the bucket ACL of the bucket in the account that will be storing the logs so that other accounts can log to it
D. Create a service-based role for CloudTrail and associate it with CloudTrail in each account
E. Update the bucket policy of the bucket in the account that will be storing the logs so that other accounts can log to it

Answer: AE

Explanation:
these are the steps that can meet the requirements in the most secure manner. CloudTrail is a service that records AWS API calls and delivers log files to an S3 bucket. Turning on CloudTrail in each IAM account can help capture all IAM API calls made within those accounts. Updating the bucket policy of the bucket in the account that will be storing the logs can help grant other accounts permission to write log files to that bucket. The other options are either unnecessary or insecure for logging and analyzing IAM API calls.

NEW QUESTION 152
A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account.
What is the MOST secure way to provide this access?

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

Answer: D

Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

NEW QUESTION 157
A company needs to encrypt all of its data stored in Amazon S3. The company wants to use IAM Key Management Service (IAM KMS) to create and manage its encryption keys. The company's security policies require the ability to Import the company's own key material for the keys, set an expiration date on the keys, and delete keys immediately, if needed.
How should a security engineer set up IAM KMS to meet these requirements?

A. Configure IAM KMS and use a custom key stor
B. Create a customer managed CMK with no key material Import the company's keys and key material into the CMK
C. Configure IAM KMS and use the default Key store Create an IAM managed CMK with no key material Import the company's key material into the CMK
D. Configure IAM KMS and use the default key store Create a customer managed CMK with no key material import the company's key material into the CMK
E. Configure IAM KMS and use a custom key stor
F. Create an IAM managed CMK with no key material.Import the company's key material into the CMK.

Answer: A

Explanation:
To meet the requirements of importing their own key material, setting an expiration date on the keys, and deleting keys immediately, the security engineer should do the following:

- Configure AWS KMS and use a custom key store. This allows the security engineer to use a key manager outside of AWS KMS that they own and manage, such as an AWS CloudHSM cluster or an external key manager.
- Create a customer managed CMK with no key material. Import the company’s keys and key material into the CMK. This allows the security engineer to use their own key material for encryption and decryption operations, and to specify an expiration date for it.

NEW QUESTION 160
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 165
A security engineer is designing a cloud architecture to support an application. The application runs on Amazon EC2 instances and processes sensitive information, including credit card numbers.
The application will send the credit card numbers to a component that is running in an isolated environment. The component will encrypt, store, and decrypt the numbers.
The component then will issue tokens to replace the numbers in other parts of the application.
The component of the application that manages the tokenization process will be deployed on a separate set of EC2 instances. Other components of the application must not be able to store or access the credit card numbers.
Which solution will meet these requirements?

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

Answer: D

Explanation:
AWS Nitro Enclaves are isolated and hardened virtual machines that run on EC2 instances and provide a secure environment for processing sensitive data. Nitro Enclaves have no persistent storage, interactive access, or external networking, and they can only communicate with the parent instance through a secure local channel. Nitro Enclaves also support cryptographic attestation, which allows verifying the identity and integrity of the enclave and its code. Nitro Enclaves are ideal for implementing data protection solutions such as tokenization, encryption, and key management.
Using Nitro Enclaves for the tokenization component of the application meets the requirements of isolating the sensitive data from other parts of the application, encrypting and storing the credit card numbers securely, and issuing tokens to replace the numbers. Other components of the application will not be able to access or store the credit card numbers, as they are only available within the enclave.

NEW QUESTION 170
A security engineer wants to evaluate configuration changes to a specific AWS resource to ensure that the resource meets compliance standards. However, the security engineer is concerned about a situation in which several configuration changes are made to the resource in quick succession. The security engineer wants to record only the latest configuration of that resource to indicate the cumulative impact of the set of changes.
Which solution will meet this requirement in the MOST operationally efficient way?

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

Answer: B

Explanation:
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.
To evaluate configuration changes to a specific AWS resource and ensure that it meets compliance standards, the security engineer should use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes. This will allow the security engineer to view the current state of the resource and its compliance status, as well as its configuration history and timeline.
AWS Config records configuration changes as ConfigurationItems, which are point-in-time snapshots of the resource's attributes, relationships, and metadata. If multiple configuration changes occur within a short period of time, AWS Config records only the latest ConfigurationItem for that resource. This indicates the cumulative impact of the set of changes on the resource's configuration.
This solution will meet the requirement in the most operationally efficient way, as it leverages AWS Config's features to monitor, record, and evaluate resource configurations without requiring additional tools or services.
The other options are incorrect because they either do not record the latest configuration in case of multiple configuration changes (A, C), or do not use a valid service for evaluating resource configurations (D).
Verified References:

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

NEW QUESTION 172
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 174
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 178
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 181
A security team is using Amazon EC2 Image Builder to build a hardened AMI with forensic capabilities. An AWS Key Management Service (AWS KMS) key will encrypt the forensic AMI EC2 Image Builder successfully installs the required patches and packages in the security team's AWS account. The security team uses a federated IAM role m the same AWS account to sign in to the AWS Management Console and attempts to launch the forensic AMI. The EC2 instance launches and immediately terminates.
What should the security learn do lo launch the EC2 instance successfully

A. Update the policy that is associated with the federated IAM role to allow the ec2. Describelmages action for the forensic AMI.
B. Update the policy that is associated with the federated IAM role to allow the ec2 Start Instances action m the security team's AWS account.
C. Update the policy that is associated with the KMS key that is used to encrypt the forensic AM
D. Configure the policy to allow the km
E. Encrypt and kms Decrypt actions for the federated IAM role.
F. Update the policy that is associated with the federated IAM role to allow the km
G. DescribeKey action for the KMS key that is used to encrypt the forensic AMI.

Answer: C

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

NEW QUESTION 183
A company that uses AWS Organizations is migrating workloads to AWS. The compa-nys application team determines that the workloads will use Amazon EC2 instanc-es, Amazon S3 buckets, Amazon DynamoDB tables, and Application Load Balancers. For each resource type, the company mandates that deployments must comply with the following requirements:
• All EC2 instances must be launched from approved AWS accounts.
• All DynamoDB tables must be provisioned with a standardized naming convention.
• All infrastructure that is provisioned in any accounts in the organization must be deployed by AWS CloudFormation templates.
Which combination of steps should the application team take to meet these re-quirements? (Select TWO.)

A. Create CloudFormation templates in an administrator AWS accoun
B. Share the stack sets with an application AWS accoun
C. Restrict the template to be used specifically by the application AWS account.
D. Create CloudFormation templates in an application AWS accoun
E. Share the output with an administrator AWS account to review compliant resource

F. Restrict output to only the administrator AWS account.
G. Use permissions boundaries to prevent the application AWS account from provisioning specific resources unless conditions for the internal compli-ance requirements are met.
H. Use SCPs to prevent the application AWS account from provisioning specific resources unless conditions for the internal compliance requirements are met.
I. Activate AWS Config managed rules for each service in the application AWS account.

Answer: AD

NEW QUESTION 188
For compliance reasons a Security Engineer must produce a weekly report that lists any instance that does not have the latest approved patches applied. The Engineer must also ensure that no system goes more than 30 days without the latest approved updates being applied
What would the MOST efficient way to achieve these goals?

A. Use Amazon inspector to determine which systems do not have the latest patches applied, and after 30 days, redeploy those instances with the latest AMI version
B. Configure Amazon EC2 Systems Manager to report on instance patch compliance and enforce updates during the defined maintenance windows
C. Examine IAM CloudTrail togs to determine whether any instances have not restarted in the last 30 days, and redeploy those instances
D. Update the AMIs with the latest approved patches and redeploy each instance during the defined maintenance window

Answer: B

Explanation:
Amazon EC2 Systems Manager is a service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems3. You can use Systems Manager to report on instance patch compliance and enforce updates during the defined maintenance windows4. The other options are either inefficient or not feasible for achieving the goals.

NEW QUESTION 189
A company's security engineer wants to receive an email alert whenever Amazon GuardDuty, AWS Identity and Access Management Access Analyzer, or Amazon Made generate a high-severity security finding. The company uses AWS Control Tower to govern all of its accounts. The company also uses AWS Security Hub with all of the AWS service integrations turned on.
Which solution will meet these requirements with the LEAST operational overhead?

A. Set up separate AWS Lambda functions for GuardDuty, 1AM Access Analyzer, and Macie to call each service's public API to retrieve high-severity finding
B. Use Amazon Simple Notification Service (Amazon SNS) to send the email alert
C. Create an Amazon EventBridge rule to invoke the functions on a schedule.
D. Create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severit
E. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topi
F. Subscribe the desired email addresses to the SNS topic.
G. Create an Amazon EventBridge rule with a pattern that matches AWS Control Tower events with high severit
H. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topi
I. Subscribe the desired email addresses to the SNS topic.
J. Host an application on Amazon EC2 to call the GuardDuty, 1AM Access Analyzer, and Macie APIs.Within the application, use the Amazon Simple Notification Service (Amazon SNS) API to retrieve high-severity findings and to send the findings to an SNS topi
K. Subscribe the desired email addresses to the SNS topic.

Answer: B

Explanation:
The AWS documentation states that you can create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severity. You can then configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. You can subscribe the desired email addresses to the SNS topic. This method is the least operational overhead way to meet the requirements.
References: : AWS Security Hub User Guide

NEW QUESTION 193
A company needs to use HTTPS when connecting to its web applications to meet compliance requirements. These web applications run in Amazon VPC on Amazon EC2 instances behind an Application Load Balancer (ALB). A security engineer wants to ensure that the load balancer win only accept connections over port 443. even if the ALB is mistakenly configured with an HTTP listener
Which configuration steps should the security engineer take to accomplish this task?

A. Create a security group with a rule that denies Inbound connections from 0.0.0 0/0 on port 00. Attach this security group to the ALB to overwrite more permissive rules from the ALB's default securitygroup.
B. Create a network ACL that denies inbound connections from 0 0.0.0/0 on port 80 Associate the network ACL with the VPC s internet gateway
C. Create a network ACL that allows outbound connections to the VPC IP range on port 443 only.Associate the network ACL with the VPC's internet gateway.
D. Create a security group with a single inbound rule that allows connections from 0.0.0 0/0 on port 443.Ensure this security group is the only one associated with the ALB

Answer: D

Explanation:
To ensure that the load balancer only accepts connections over port 443, the security engineer should do the following:
- Create a security group with a single inbound rule that allows connections from 0.0.0.0/0 on port 443.

This means that the security group allows HTTPS traffic from any source IP address.
- Ensure this security group is the only one associated with the ALB. This means that the security group overrides any other rules that might allow HTTP traffic on port 80.

NEW QUESTION 194
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 198
Developers in an organization have moved from a standard application deployment to containers. The Security Engineer is tasked with ensuring that the containers are secure. Which strategies will reduce the attack surface and enhance the security of the containers? (Select TWO.)

A. Use the containers to automate security deployments.
B. Limit resource consumption (CPU, memory), networking connections, ports, and unnecessary container libraries.
C. Segregate containers by host, function, and data classification.
D. Use Docker Notary framework to sign task definitions.
E. Enable container breakout at the host kernel.

Answer: AC

Explanation:
these are the strategies that can reduce the attack surface and enhance the security of the containers. Containers are a method of packaging and running applications in isolated environments. Using containers to automate security deployments can help ensure that security patches and updates are applied consistently and quickly across the container fleet. Segregating containers by host, function, and data classification can help limit the impact of a compromise and enforce the principle of least privilege. The other options are either irrelevant or risky for securing containers.

NEW QUESTION 201
An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket.
A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.
What is the FASTEST way to prevent the sensitive data from being exposed?

A. Download the data from the existing S3 bucket to a new EC2 instanc
B. Then delete the data from the S3 bucke
C. Re-encrypt the data with a client-based ke
D. Upload the data to a new S3 bucket.
E. Block access to the public range of S3 endpoint IP addresses by using a host-based firewal
F. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.
G. Revoke the IAM role's active session permission
H. Update the S3 bucket policy to deny access to the IAM rol
I. Remove the IAM role from the EC2 instance profile.
J. Disable the current ke
K. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new ke
L. Schedule the compromised key for deletion.

Answer: D

NEW QUESTION 205
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C02 Product From:

https://www.2passeasy.com/dumps/SCS-C02/

Money Back Guarantee

SCS-C02 Practice Exam Features:

* SCS-C02 Questions and Answers Updated Frequently

* SCS-C02 Practice Questions Verified by Expert Senior Certified Staff

* SCS-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SCS-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year