# Amazon

## Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

**NEW QUESTION 1**
A company manages three separate IAM accounts for its production, development, and test environments, Each Developer is assigned a unique IAM user under the development account. A new application hosted on an Amazon EC2 instance in the developer account requires read access to the archived documents stored in an Amazon S3 bucket in the production account.
How should access be granted?

A. Create an IAM role in the production account and allow EC2 instances in the development account to assume that role using the trust polic
B. Provide read access for the required S3 bucket to this role.
C. Use a custom identity broker to allow Developer IAM users to temporarily access the S3 bucket.
D. Create a temporary IAM user for the application to use in the production account.
E. Create a temporary IAM user in the production account and provide read access to Amazon S3.Generate the temporary IAM user's access key and secret key and store these on the EC2 instance used by the application in the development account.

**Answer:** A

**Explanation:**
https://IAM.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/


**NEW QUESTION 2**
A company discovers a billing anomaly in its AWS account. A security consultant investigates the anomaly and discovers that an employee who left the company 30 days ago still has access to the account.
The company has not monitored account activity in the past.
The security consultant needs to determine which resources have been deployed or reconfigured by the employee as quickly as possible.
Which solution will meet these requirements?

A. In AWS Cost Explorer, filter chart data to display results from the past 30 day
B. Export the results to a data tabl
C. Group the data table by re-source.
D. Use AWS Cost Anomaly Detection to create a cost monito
E. Access the detec-tion histor
F. Set the time frame to Last 30 day
G. In the search area, choose the service category.
H. In AWS CloudTrail, filter the event history to display results from the past 30 day
I. Create an Amazon Athena table that contains the dat
J. Parti-tion the table by event source.
K. Use AWS Audit Manager to create an assessment for the past 30 day
L. Apply a usage-based framework to the assessmen
M. Configure the assessment to as-sess by resource.

**Answer:** C


**NEW QUESTION 3**
A company wants to protect its website from man in-the-middle attacks by using Amazon CloudFront. Which solution will meet these requirements with the LEAST operational overhead?

A. Use the SimpleCORS managed response headers policy.
B. Use a Lambda@Edge function to add the Strict-Transport-Security response header.
C. Use the SecurityHeadersPolicy managed response headers policy.
D. Include the X-XSS-Protection header in a custom response headers policy.

**Answer:** C

**Explanation:**
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-managed-response-headers-poli The SecurityHeadersPolicy is a managed policy provided by Amazon CloudFront that includes a set of recommended security headers to enhance the security of your website. These headers help protect against various types of attacks, including man-in-the-middle attacks. By applying the SecurityHeadersPolicy to your CloudFront distribution, the necessary security headers will be automatically added to the responses sent by CloudFront. This reduces operational overhead because you don't have to manually configure or manage the headers yourself.


**NEW QUESTION 4**
A company wants to prevent SSH access through the use of SSH key pairs for any Amazon Linux 2 Amazon EC2 instances in its AWS account. However, a system administrator occasionally will need to access these EC2 instances through SSH in an emergency. For auditing purposes, the company needs to record any commands that a user runs in an EC2 instance.
What should a security engineer do to configure access to these EC2 instances to meet these requirements?

A. Use the EC2 serial console Configure the EC2 serial console to save all commands that are entered to an Amazon S3 bucke
B. Provide the EC2 instances with an IAM role that allows the EC2 serial console to access Amazon S3. Configure an IAM account for the system administrato
C. Provide an IAM policy that allows the IAM account to use the EC2 serial console.
D. Use EC2 Instance Connect Configure EC2 Instance Connect to save all commands that are entered to Amazon CloudWatch Log
E. Provide the EC2 instances with an IAM role that allows the EC2 instances to access CloudWatch Logs Configure an IAM account for the system administrato
F. Provide an IAM policy that allows the IAM account to use EC2 Instance Connect.
G. Use an EC2 key pair with an EC2 instance that needs SSH access Access the EC2 instance with this key pair by using SS
H. Configure the EC2 instance to save all commands that are entered to Amazon CloudWatch Log
I. Provide the EC2 instance with an IAM role that allows the EC2 instance to access Amazon S3 and CloudWatch Logs.
J. Use AWS Systems Manager Session Manager Configure Session Manager to save all commands that are entered in a session to an Amazon S3 bucke
K. Provide the EC2 instances with an IAM role that allows Systems Manager to manage the EC2 instance
L. Configure an IAM account for the system administrator Provide an IAM policy that allows the IAM account to use Session Manager.

**Answer:** D

**Explanation:**
Open the AWS Systems Manager console at https://console.aws.amazon.com/systems-manager/. In the navigation pane, choose Session Manager. Choose the Preferences tab, and then choose Edit. Select the check box next to Enable under S3 logging. (Recommended) Select the check box next to Allow only encrypted S3 buckets. With this option turned on, log data is encrypted using the server-side encryption key specified for the bucket. If you don't want to encrypt the log data that is sent to Amazon S3, clear the check box. You must also clear the check box if encryption isn't allowed on the S3 bucket.

**NEW QUESTION 5**
A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.
A security engineer must automate a response in the company's organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company's security team.
Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

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

**Answer:** ACF

**Explanation:**
The correct answer is A, C, and F.
To automate a response for any newly created policies that are overly permissive, the security engineer needs to use a combination of services that can monitor, analyze, remediate, and notify the security incidents.
Option A is correct because creating an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role is a valid way to remediate external access. AWS Step Functions is a service that allows you to coordinate multiple AWS services into serverless workflows. You can use Step Functions to invoke AWS Lambda functions, which can modify the IAM policies programmatically. You can also use Step Functions to publish a notification to an Amazon SNS topic, which can send messages to subscribers such as email addresses.
Option B is incorrect because creating an AWS Batch job that forwards any resource type findings to an AWS Lambda function is not a suitable way to automate a response. AWS Batch is a service that enables you to run batch computing workloads on AWS. Batch is designed for large-scale and long-running jobs that can benefit from parallelization and dynamic provisioning of compute resources. Batch is not intended for event-driven and real-time workflows that require immediate response.
Option C is correct because creating an Amazon EventBridge event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution is a valid way to monitor and analyze the security incidents. Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from various sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke AWS Step Functions state machines from the IAM Access Analyzer findings.
Option D is incorrect because creating an Amazon CloudWatch metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution is not a suitable way to monitor and analyze the security incidents. Amazon CloudWatch is a service that provides monitoring and observability for your AWS resources and applications. CloudWatch can collect metrics, logs, and events from various sources and perform actions based on alarms or filters. However, CloudWatch cannot directly invoke AWS Batch jobs from the IAM Access Analyzer findings. You would need to use another service such as EventBridge or SNS to trigger the Batch job.
Option E is incorrect because creating an Amazon SQS queue that forwards a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked is not a valid way to notify the security incidents. Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS can deliver messages to consumers that poll the queue for messages. However, SQS cannot directly forward a notification to the security team's email addresses. You would need to use another service such as SNS or SES to send email notifications.
Option F is correct because creating an Amazon SNS topic for external or cross-account access notices and subscribing the security team's email addresses to the topic is a valid way to notify the security incidents. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can use SNS to send email notifications to the security team when a critical security finding is detected.
References:
- AWS Step Functions
- AWS Batch
- Amazon EventBridge
- Amazon CloudWatch
- Amazon SQS
- Amazon SNS

**NEW QUESTION 6**
A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region. The DB cluster is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. To meet compliance requirements, the company needs to copy a DB snapshot to the us-west-1 Region. However, when the company tries to copy the snapshot to us-west-1 the company cannot access the key that was used to encrypt the original database.
What should the company do to set up the snapshot in us-west-1 with proper encryption?

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

**Answer:** B

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

**NEW QUESTION 7**
A security engineer wants to use Amazon Simple Notification Service (Amazon SNS) to send email alerts to a company's security team for Amazon GuardDuty findings
that have a High severity level. The security engineer also wants to deliver these findings to a visualization tool for further examination.
Which solution will meet these requirements?

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

**Answer:** C

**NEW QUESTION 8**
A company has a large fleet of Linux Amazon EC2 instances and Windows EC2 instances that run in private subnets. The company wants all remote administration to be performed as securely as possible in the AWS Cloud.
Which solution will meet these requirements?

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

**Answer:** A

**Explanation:**
AWS Systems Manager Session Manager is a fully managed service that allows you to securely and remotely administer your EC2 instances without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager provides an interactive browser-based shell or CLI access to your instances, as well as port forwarding and auditing capabilities. Session Manager works with both Linux and Windows instances, and supports hybrid environments and edge devices.
EC2 Instance Connect is a feature that allows you to use SSH to connect to your Linux instances using
short-lived keys that are generated on demand and delivered securely through the AWS metadata service. EC2 Instance Connect does not require any additional software installation or configuration on the instance, but it does require you to use SSH-RSA keys during the launch of new instances.
The correct answer is to use Session Manager, as it provides more security and flexibility than EC2 Instance Connect, and does not require SSH-RSA keys or inbound ports. Session Manager also works with Windows instances, while EC2 Instance Connect does not.
Verified References:
> https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html
> https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html
> https://repost.aws/questions/QUnV4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec-2-ins

**NEW QUESTION 9**
A recent security audit found that IAM CloudTrail logs are insufficiently protected from tampering and unauthorized access Which actions must the Security Engineer take to address these audit findings? (Select THREE )

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

F. Encrypt the CloudTrail log files with server-side encryption with IAM KMS-managed keys (SSE-KMS)

**Answer:** ADE

**NEW QUESTION 10**
A company wants to establish separate IAM Key Management Service (IAM KMS) keys to use for different IAM services. The company's security engineer created the following key policy lo allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role:

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

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

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

**Answer:** C

**Explanation:**
To resolve the issues, the security engineer should make the following change to the policy:

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

**NEW QUESTION 10**
A company is expanding its group of stores. On the day that each new store opens, the company wants to launch a customized web application for that store. Each store's application will have a non-production environment and a production environment. Each environment will be deployed in a separate AWS account. The company uses AWS Organizations and has an OU that is used only for these accounts.
The company distributes most of the development work to third-party development teams. A security engineer needs to ensure that each team follows the company's
deployment plan for AWS resources. The security engineer also must limit access to the deployment plan to only the developers who need access. The security engineer already has created an AWS CloudFormation template that implements the deployment plan.
What should the security engineer do next to meet the requirements in the MOST secure way?

A. Create an AWS Service Catalog portfolio in the organization's management accoun
B. Upload the CloudFormation templat
C. Add the template to the portfolio's product lis
D. Share the portfolio with the OIJ.
E. Use the CloudFormation CLI to create a module from the CloudFormation templat
F. Register the module as a private extension in the CloudFormation registr
G. Publish the extensio
H. In the OU, create an SCP that allows access to the extension.
I. Create an AWS Service Catalog portfolio in the organization's management accoun

J. Upload the CloudFormation templat
K. Add the template to the portfolio's product lis
L. Create an IAM role that has a trust policy that allows cross-account access to the portfolio for users in the OU account
M. Attach the AWSServiceCatalogEndUserFullAccess managed policy to the role.
N. Use the CloudFormation CLI to create a module from the CloudFormation templat
O. Register the module as a private extension in the CloudFormation registr
P. Publish the extensio
Q. Share the extension with the OU

**Answer:** A

**Explanation:**
The correct answer is A. Create an AWS Service Catalog portfolio in the organization's management account. Upload the CloudFormation template. Add the template to the portfolio's product list. Share the portfolio with the OU.
According to the AWS documentation, AWS Service Catalog is a service that allows you to create and manage catalogs of IT services that are approved for use on AWS. You can use Service Catalog to centrally manage commonly deployed IT services and help achieve consistent governance and compliance requirements, while enabling users to quickly deploy only the approved IT services they need.
To use Service Catalog with multiple AWS accounts, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use Service Catalog as a service principal for AWS Organizations, which lets you share your portfolios with organizational units (OUs) or accounts in your organization.
To create a Service Catalog portfolio, you need to use an administrator account, such as the organization's management account. You can upload your CloudFormation template as a product in your portfolio, and define constraints and tags for it. You can then share your portfolio with the OU that contains the accounts for the web applications. This will allow the developers in those accounts to launch products from the shared portfolio using the Service Catalog end user console.
Option B is incorrect because CloudFormation modules are reusable components that encapsulate one or more resources and their configurations. They are not meant to be used as templates for deploying entire stacks of resources. Moreover, sharing a module with an OU does not grant access to launch stacks from it.
Option C is incorrect because creating an IAM role that has a trust policy that allows cross-account access to the portfolio is not secure. It would allow any user in the OU accounts to assume the role and access the portfolio, regardless of their job function or access requirements.
Option D is incorrect because sharing a module with an OU does not grant access to launch stacks from it. It also does not limit access to the deployment plan to only the developers who need access.

**NEW QUESTION 12**
A company has a batch-processing system that uses Amazon S3, Amazon EC2, and AWS Key Management Service (AWS KMS). The system uses two AWS accounts: Account A and Account B.
Account A hosts an S3 bucket that stores the objects that will be processed. The S3 bucket also stores the results of the processing. All the S3 bucket objects are encrypted by a KMS key that is managed in
Account A.
Account B hosts a VPC that has a fleet of EC2 instances that access the S3 buck-et in Account A by using statements in the bucket policy. The VPC was created with DNS hostnames enabled and DNS resolution enabled.
A security engineer needs to update the design of the system without changing any of the system's code. No AWS API calls from the batch-processing EC2 in-stances can travel over the internet.
Which combination of steps will meet these requirements? (Select TWO.)

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

**Answer:** BC

**NEW QUESTION 14**
A System Administrator is unable to start an Amazon EC2 instance in the eu-west-1 Region using an IAM role The same System Administrator is able to start an EC2 instance in the eu-west-2 and eu-west-3 Regions. The IAMSystemAdministrator access policy attached to the System Administrator IAM role allows unconditional access to all IAM services and resources within the account
Which configuration caused this issue?
A) An SCP is attached to the account with the following permission statement:

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

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

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

C)

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

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

D)

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

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

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

**Answer:** B

## NEW QUESTION 18

An organization has a multi-petabyte workload that it is moving to Amazon S3, but the CISO is concerned about cryptographic wear-out and the blast radius if a key is compromised. How can the CISO be assured that IAM KMS and Amazon S3 are addressing the concerns? (Select TWO )

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

**Answer:** CE

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

## NEW QUESTION 20

A security engineer receives an IAM abuse email message. According to the message, an Amazon EC2 instance that is running in the security engineer's IAM account is sending phishing email messages.
The EC2 instance is part of an application that is deployed in production. The application runs on many EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple subnets and multiple Availability Zones.
The instances normally communicate only over the HTTP. HTTPS, and MySQL protocols. Upon investigation, the security engineer discovers that email messages are being sent over port 587. All other traffic is normal.
The security engineer must create a solution that contains the compromised EC2 instance, preserves forensic evidence for analysis, and minimizes application downtime. Which combination of steps must the security engineer take to meet these requirements? (Select THREE.)

A. Add an outbound rule to the security group that is attached to the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.
B. Add an outbound rule to the network ACL for the subnet that contains the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.
C. Gather volatile memory from the compromised EC2 instanc
D. Suspend the compromised EC2 instance from the Auto Scaling grou
E. Then take a snapshot of the compromised EC2 instanc
F. v
G. Take a snapshot of the compromised EC2 instanc
H. Suspend the compromised EC2 instance from the Auto Scaling grou
I. Then gather volatile memory from the compromised EC2 instance.
J. Move the compromised EC2 instance to an isolated subnet that has a network ACL that has no inbound rules or outbound rules.
K. Replace the existing security group that is attached to the compromised EC2 instance with a new security group that has no inbound rules or outbound rules.

**Answer:** ACE

## NEW QUESTION 24

A company's Security Engineer is copying all application logs to centralized Amazon S3 buckets. Currently, each of the company's applications is in its own IAM account, and logs are pushed into S3 buckets associated with each account. The Engineer will deploy an IAM Lambda function into each account that copies the relevant log files to the centralized S3 bucket.
The Security Engineer is unable to access the log files in the centralized S3 bucket. The Engineer's IAM user policy from the centralized account looks like this:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:Put*",
            "Resource":"arn:aws:s3:::centralizedbucket/*",
            "Effect": "Deny"
        },
        {
            "Action": ["s3:Get*","s3:List*"],
            "Resource": [
                "arn:aws:s3:::centralizedbucket/*",
                "arn:aws:s3:::centralizedbucket/"
            ],
            "Effect": "Allow"
        }
    ]
}
```

The centralized S3 bucket policy looks like this:

```
{
    "Version": "2012-10-17",    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/LogCopier",
                    "arn:aws:iam::444455556666:role/LogCopier"
                ]
            },
            "Action": ["s3:PutObject","s3:PutObjectAcl"],
            "Resource": "arn:aws:s3:::centralizedbucket/*"
        }
    ]
}
```

Why is the Security Engineer unable to access the log files?

A. The S3 bucket policy does not explicitly allow the Security Engineer access to the objects in the bucket.
B. The object ACLs are not being updated to allow the users within the centralized account to access the objects
C. The Security Engineers IAM policy does not grant permissions to read objects in the S3 bucket
D. The s3:PutObject and s3:PutObjectAcl permissions should be applied at the S3 bucket level

**Answer:** C


**NEW QUESTION 28**
A company finds that one of its Amazon EC2 instances suddenly has a high CPU usage. The company does not know whether the EC2 instance is compromised or whether the operating system is performing background cleanup.
Which combination of steps should a security engineer take before investigating the issue? (Select THREE.)

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

**Answer:** BCE

**Explanation:**
https://d1.awsstatic.com/WWPS/pdf/aws_security_incident_response.pdf


**NEW QUESTION 31**
A company has two AWS accounts. One account is for development workloads. The other account is for production workloads. For compliance reasons the production account contains all the AWS Key Management. Service (AWS KMS) keys that the company uses for encryption.
The company applies an IAM role to an AWS Lambda function in the development account to allow secure access to AWS resources. The Lambda function must access a specific KMS customer managed key that exists in the production account to encrypt the Lambda function's data.
Which combination of steps should a security engineer take to meet these requirements? (Select TWO.)

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

G. Configure the IAM role for the Lambda function in the development account by attaching an IAM policy that allows access to the customer managed key in the production account.

**Answer:** BE

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

≫ Configure the key policy for the customer managed key in the production account to allow access to the IAM role of the Lambda function in the development account. A key policy is a resource-based policy that defines who can use or manage a KMS key. To grant cross-account access to a KMS key, you must specify the AWS account ID and the IAM role ARN of the external principal in the key policy statement. For more information, see Allowing users in other accounts to use a KMS key.

≫ Configure the IAM role for the Lambda function in the development account by attaching an IAM policy that allows access to the customer managed key in the production account. An IAM policy is an identity-based policy that defines what actions an IAM entity can perform on which resources. To allow an IAM role to use a KMS key in another account, you must specify the KMS key ARN and the kms:Encrypt action (or any other action that requires access to the KMS key) in the IAM policy statement. For more information, see Using IAM policies with AWS KMS.
This solution will meet the requirements of allowing secure access to a KMS customer managed key across AWS accounts.
The other options are incorrect because they either do not grant cross-account access to the KMS key (A, C), or do not use a valid policy type for KMS keys (D).
Verified References:

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

**NEW QUESTION 34**
Your company has a set of EC2 Instances defined in IAM. These Ec2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly. How can you achieve this?
Please select:

A. Use Cloudwatch logs to monitor the activity on the Security Group
B. Use filters to search for the changes and use SNS for the notification.
C. Use Cloudwatch metrics to monitor the activity on the Security Group
D. Use filters to search for the changes and use SNS for the notification.
E. Use IAM inspector to monitor the activity on the Security Group
F. Use filters to search for the changes and use SNS f the notification.
G. Use Cloudwatch events to be triggered for any changes to the Security Group
H. Configure the Lambda function for email notification as well.

**Answer:** D

**Explanation:**
The below diagram from an IAM blog shows how security groups can be monitored
C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A is invalid because you need to use Cloudwatch Events to check for chan, Option B is invalid because you need to use Cloudwatch Events to check for chang
Option C is invalid because IAM inspector is not used to monitor the activity on Security Groups For more information on monitoring security groups, please visit the below URL:
Ihttpsy/IAM.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notifications-about-changes-t 'pc-security-groups/
The correct answer is: Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.
Submit your Feedback/Queries to our Experts

**NEW QUESTION 38**
A security engineer configures Amazon S3 Cross-Region Replication (CRR) for all objects that are in an S3 bucket in the us-east-1. Region Some objects in this S3 bucket use server-side encryption with AWS KMS keys (SSE-KMS) for encryption at test. The security engineer creates a destination S3 bucket in the us-west-2 Region. The destination S3 bucket is in the same AWS account as the source S3 bucket.
The security engineer also creates a customer managed key in us-west-2 to encrypt objects at rest in the destination S3 bucket. The replication configuration is set to use the key in us-west-2 to encrypt objects in the destination S3 bucket. The security engineer has provided the S3 replication configuration with an IAM role to perform the replication in Amazon S3.
After a day, the security engineer notices that no encrypted objects from the source S3 bucket are replicated to the destination S3 bucket. However, all the unencrypted objects are replicated.
Which combination of steps should the security engineer take to remediate this issue? (Select THREE.)

A. Change the replication configuration to use the key in us-east-1 to encrypt the objects that are in the destination S3 bucket.
B. Grant the IAM role the km
C. Encrypt permission for the key in us-east-1 that encrypts source objects.
D. Grant the IAM role the s3 GetObjectVersionForReplication permission for objects that are in the source S3 bucket.
E. Grant the IAM role the km
F. Decrypt permission for the key in us-east-1 that encrypts source objects.
G. Change the key policy of the key in us-east-1 to grant the km
H. Decrypt permission to the security engineer's IAM account.
I. Grant the IAM role the kms Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket.

**Answer:** BF

**Explanation:**
To enable S3 Cross-Region Replication (CRR) for objects that are encrypted with SSE-KMS, the following steps are required:

> Grant the IAM role the kms.Decrypt permission for the key in us-east-1 that encrypts source objects.
This will allow the IAM role to decrypt the source objects before replicating them to the destination bucket. The kms.Decrypt permission must be granted in the key policy of the source KMS key or in an IAM policy attached to the IAM role.

> Grant the IAM role the kms.Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket. This will allow the IAM role to encrypt the replica objects with the destination KMS key before storing them in the destination bucket. The kms.Encrypt permission must be granted in the key policy of the destination KMS key or in an IAM policy attached to the IAM role.
This solution will remediate the issue of encrypted objects not being replicated to the destination bucket.
The other options are incorrect because they either do not grant the necessary permissions for CRR (A, C, D), or do not use a valid encryption method for CRR (E).
Verified References:

> https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html


**NEW QUESTION 40**
While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139).
The ping command did not return a response. The flow log in the VPC showed the following:
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
What action should be performed to allow the ping to work?

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

**Answer:** D


**NEW QUESTION 44**
A company stores images for a website in an Amazon S3 bucket. The company is using Amazon CloudFront to serve the images to end users. The company recently discovered that the images are being accessed from countries where the company does not have a distribution license.
Which actions should the company take to secure the images to limit their distribution? (Select TWO.)

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

**Answer:** AC

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

> Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI). This allows the company to use a special CloudFront user that can access objects in their S3 bucket, and prevent anyone else from accessing them directly.

> Add a CloudFront geo restriction deny list of countries where the company lacks a license. This allows the company to use a feature that controls access to their content based on the geographic location of their viewers, and block requests from countries where they do not have a distribution license.


**NEW QUESTION 45**
A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.
Which solution will meet these requirements with the LEAST management overhead?

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

L. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
M. Pull images from the public container registr
N. Publish the images to AWS CodeArtifact repositories in a centralized AWS accoun
O. Use a CI/CD pipeline to deploy the images to different AWS account
P. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

**Answer:** C

**Explanation:**
The correct answer is C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account.
Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
This solution meets the requirements because:

≫ Amazon ECR is a fully managed container registry service that supports Docker and OCI images and artifacts1. It integrates with Amazon ECS and other AWS services to simplify the development and deployment of container-based applications.

≫ Amazon ECR provides image scanning on push, which uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project to detect software vulnerabilities in container images2. The scan results are available in the AWS Management Console, AWS CLI, or AWS SDKs2.

≫ Amazon ECR supports cross-account access to repositories, which allows sharing images across multiple AWS accounts3. This can be achieved by using repository policies, which are resource-based policies that specify which IAM principals and accounts can access the repositories and what actions they can perform4. Additionally, identity-based policies can be used to control which IAM roles in each account can access the repositories5.
The other options are incorrect because:

≫ A. This option does not use repository policies to restrict cross-account access to the images, which is a requirement. Identity-based policies alone are not sufficient to control access to Amazon ECR repositories5.

≫ B. This option does not use Amazon ECR, which is a fully managed service that provides image scanning and cross-account access features. Hosting a private container registry on EC2 instances would require more management overhead and additional security measures.

≫ D. This option uses AWS CodeArtifact, which is a fully managed artifact repository service that supports Maven, npm, NuGet, PyPI, and generic package formats6. However, AWS CodeArtifact does not support Docker or OCI container images, which are required for Amazon ECS applications.


**NEW QUESTION 47**
Amazon GuardDuty has detected communications to a known command and control endpoint from a company's Amazon EC2 instance. The instance was found to be running a vulnerable version of a common web framework. The company's security operations team wants to quickly identity other compute resources with the specific version of that framework installed.
Which approach should the team take to accomplish this task?

A. Scan all the EC2 instances for noncompliance with IAM Confi
B. Use Amazon Athena to query IAM CloudTrail logs for the framework installation
C. Scan all the EC2 instances with the Amazon Inspector Network Reachability rules package to identity instances running a web server with RecognizedPortWithListener findings
D. Scan all the EC2 instances with IAM Systems Manager to identify the vulnerable version of the web framework
E. Scan an the EC2 instances with IAM Resource Access Manager to identify the vulnerable version of the web framework

**Answer:** C

**Explanation:**
To quickly identify other compute resources with the specific version of the web framework installed, the team should do the following:

≫ Scan all the EC2 instances with AWS Systems Manager to identify the vulnerable version of the web framework. This allows the team to use AWS Systems Manager Inventory to collect and query
information about the software installed on their EC2 instances, and to filter the results by software name and version.


**NEW QUESTION 50**
A company has an application that uses dozens of Amazon DynamoDB tables to store data. Auditors find that the tables do not comply with the company's data protection policy.
The company's retention policy states that all data must be backed up twice each month: once at midnight on the 15th day of the month and again at midnight on the 25th day of the month. The company must retain the backups for 3 months.
Which combination of steps should a security engineer take to meet these re-quirements? (Select TWO.)

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

**Answer:** AD


**NEW QUESTION 55**
A company has an application that uses an Amazon RDS PostgreSQL database. The company is developing an application feature that will store sensitive information for an individual in the database.
During a security review of the environment, the company discovers that the RDS DB instance is not encrypting data at rest. The company needs a solution that will provide encryption at rest for all the existing data and for any new data that is entered for an individual.
Which combination of options can the company use to meet these requirements? (Select TWO.)

A. Create a snapshot of the DB instanc
B. Copy the snapshot to a new snapshot, and enable encryption for the copy proces
C. Use the new snapshot to restore the DB instance.
D. Modify the configuration of the DB instance by enabling encryptio
E. Create a snapshot of the DB instanc
F. Use the snapshot to restore the DB instance.
G. Use IAM Key Management Service (IAM KMS) to create a new default IAM managed awa/rds key.Select this key as the encryption key for operations with Amazon RDS.
H. Use IAM Key Management Service (IAM KMS] to create a new CM
I. Select this key as the encryption key for operations with Amazon RDS.
J. Create a snapshot of the DB instanc
K. Enable encryption on the snapshoVUse the snapshot to restore the DB instance.

**Answer:** CE

**NEW QUESTION 56**
A company in France uses Amazon Cognito with the Cognito Hosted Ul as an identity broker for sign-in and sign-up processes. The company is marketing an application and expects that all the application's users will come from France.
When the company launches the application the company's security team observes fraudulent sign-ups for the application. Most of the fraudulent registrations are from users outside of France.
The security team needs a solution to perform custom validation at sign-up Based on the results of the validation the solution must accept or deny the registration request.
Which combination of steps will meet these requirements? (Select TWO.)

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

**Answer:** B

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

**NEW QUESTION 59**
A security engineer needs to develop a process to investigate and respond to po-tential security events on a company's Amazon EC2 instances. All the EC2 in-stances are backed by Amazon Elastic Block Store (Amazon EBS). The company uses AWS Systems Manager to manage all the EC2 instances and has installed Systems Manager Agent (SSM Agent) on all the EC2 instances.
The process that the security engineer is developing must comply with AWS secu-rity best practices and must meet the following requirements:
• A compromised EC2 instance's volatile memory and non-volatile memory must be preserved for forensic purposes.
• A compromised EC2 instance's metadata must be updated with corresponding inci-dent ticket information.
• A compromised EC2 instance must remain online during the investigation but must be isolated to prevent the spread of malware.
• Any investigative activity during the collection of volatile data must be cap-tured as part of the process. Which combination of steps should the security engineer take to meet these re-quirements with the LEAST
operational overhead? (Select THREE.)

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

**Answer:** ACE

**NEW QUESTION 63**
A company has a relational database workload that runs on Amazon Aurora MySQL. According to new compliance standards the company must rotate all database credentials every 30 days. The company needs a solution that maximizes security and minimizes development effort.
Which solution will meet these requirements?

A. Store the database credentials in AWS Secrets Manage
B. Configure automatic credential rotation tor every 30 days.
C. Store the database credentials in AWS Systems Manager Parameter Stor
D. Create an AWS Lambda function to rotate the credentials every 30 days.
E. Store the database credentials in an environment file or in a configuration fil

F. Modify the credentials every 30 days.
G. Store the database credentials in an environment file or in a configuration fil
H. Create an AWS Lambda function to rotate the credentials every 30 days.

**Answer:** A

**Explanation:**
To rotate database credentials every 30 days, the most secure and efficient solution is to store the database credentials in AWS Secrets Manager and configure automatic credential rotation for every 30 days. Secrets Manager can handle the rotation of the credentials in both the secret and the database, and it can use AWS KMS to encrypt the credentials. Option B is incorrect because it requires creating a custom Lambda function to rotate the credentials, which is more effort than using Secrets Manager. Option C is incorrect because it stores the database credentials in an environment file or a configuration file, which is less secure than using Secrets Manager. Option D is incorrect because it combines the drawbacks of option B and option C. Verified References:

➢ https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html

➢ https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_turn-on-for-other.html

**NEW QUESTION 66**
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 67**
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 72**
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 74**
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 77**
A Security Architect has been asked to review an existing security architecture and identify why the application servers cannot successfully initiate a connection to the database servers. The following summary describes the architecture:
* 1 An Application Load Balancer, an internet gateway, and a NAT gateway are configured in the public subnet
* 2. Database, application, and web servers are configured on three different private subnets.
* 3 The VPC has two route tables: one for the public subnet and one for all other subnets The route table for the public subnet has a 0 0 0 0/0 route to the internet gateway The route table for all other subnets has a 0 0.0.0/0 route to the NAT gateway. All private subnets can route to each other
* 4 Each subnet has a network ACL implemented that limits all inbound and outbound connectivity to only the required ports and protocols
* 5 There are 3 Security Groups (SGs) database application and web Each group limits all inbound and outbound connectivity to the minimum required
Which of the following accurately reflects the access control mechanisms the Architect should verify1?

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

**Answer:** A

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

**NEW QUESTION 81**
A company uses a third-party identity provider and SAML-based SSO for its AWS accounts. After the third-party identity provider renewed an expired signing certificate, users saw the following message when trying to log in:
Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)
A security engineer needs to provide a solution that corrects the error and min-imizes operational overhead.
Which solution meets these requirements?

A. Upload the third-party signing certificate's new private key to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS Management Console.
B. Sign the identity provider's metadata file with the new public ke
C. Upload the signature to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CU.
D. Download the updated SAML metadata file from the identity service provid-e
E. Update the file in the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI.
F. Configure the AWS identity provider entity defined in AWS Identity and Ac-cess Management (IAM) to synchronously fetch the new public key by using the AWS Management Console.

**Answer:** C

**Explanation:**
This answer is correct because downloading the updated SAML metadata file from the identity service provider ensures that AWS has the latest information about the identity provider, including the new public key. Updating the file in the AWS identity provider entity defined in IAM by using the AWS CLI allows AWS to verify the signature of the SAML assertions sent by the identity provider. This solution also minimizes operational overhead because it can be automated with a script or a cron job.

**NEW QUESTION 83**
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 86**
A corporation is preparing to acquire several companies. A Security Engineer must design a solution to ensure that newly acquired IAM accounts follow the corporation's security best practices. The solution should monitor each Amazon S3 bucket for unrestricted public write access and use IAM managed services.
What should the Security Engineer do to meet these requirements?

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

**Answer:** C

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

**NEW QUESTION 87**
A company uses SAML federation to grant users access to AWS accounts. A company workload that is in an isolated AWS account runs on immutable infrastructure with no human access to Amazon EC2. The company requires a specialized user known as a break glass user to have access to the workload AWS account and instances in the case of SAML errors. A recent audit discovered that the company did not create the break glass user for the AWS account that contains the workload.
The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team.
Which combination of solutions will meet these requirements? (Select TWO.)

A. Create a local individual break glass IAM user for the security tea
B. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned o
C. Use Amazon EventBridge to monitor local user activities.
D. Create a break glass EC2 key pair for the AWS accoun
E. Provide the key pair to the security tea
F. Use AWS CloudTrail to monitor key pair activit
G. Send notifications to the security team by using Amazon Simple Notification Service (Amazon SNS).
H. Create a break glass IAM role for the accoun
I. Allow security team members to perform the AssumeRoleWithSAML operatio
J. Create an AWS Cloud Trail trail that has Amazon CloudWatch Logs turned o
K. Use Amazon EventBridge to monitor security team activities.

L. Create a local individual break glass IAM user on the operating system level of each workload instance.Configure unrestricted security groups on the instances to grant access to the break glass IAM users.
M. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS Cloud Trail filter based on Session Manage
N. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic.

**Answer:** AE

**Explanation:**
The combination of solutions that will meet the requirements are:

≫ A. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities. This is a valid solution because it allows the security team to access the workload AWS account and instances using a local IAM user that does not depend on SAML federation. It also enables logging and monitoring of the break glass user activities using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon EventBridge123.

≫ E. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic. This is a valid solution because it allows the security team to access the workload instances without opening any inbound ports or managing SSH keys or bastion hosts. It also enables logging and notification of the break glass user activities using AWS CloudTrail, Session Manager, and Amazon SNS456.
The other options are incorrect because:

≫ B. Creating a break glass EC2 key pair for the AWS account and providing it to the security team is not a valid solution, because it requires opening inbound ports on the instances and managing SSH keys, which increases the security risk and complexity7.

≫ C. Creating a break glass IAM role for the account and allowing security team members to perform the AssumeRoleWithSAML operation is not a valid solution, because it still depends on SAML federation, which might not work in case of SAML errors8.

≫ D. Creating a local individual break glass IAM user on the operating system level of each workload instance and configuring unrestricted security groups on the instances to grant access to the break glass IAM users is not a valid solution, because it requires opening inbound ports on the instances and managing multiple local users, which increases the security risk and complexity9.
References:
1: Creating an IAM User in Your AWS Account 2: Creating a Trail - AWS CloudTrail 3: Using Amazon EventBridge with AWS CloudTrail 4: Setting up Session Manager - AWS Systems Manager 5: Logging Session Manager sessions - AWS Systems Manager 6: Amazon Simple Notification Service 7: Connecting to your Linux instance using SSH - Amazon Elastic Compute Cloud 8: AssumeRoleWithSAML - AWS Security Token Service 9: IAM Users - AWS Identity and Access Management

**NEW QUESTION 90**
An Incident Response team is investigating an IAM access key leak that resulted in Amazon EC2 instances being launched. The company did not discover the incident until many months later The Director of Information Security wants to implement new controls that will alert when similar incidents happen in the future
Which controls should the company implement to achieve this? {Select TWO.)

A. Enable VPC Flow Logs in all VPCs Create a scheduled IAM Lambda function that downloads and parses the logs, and sends an Amazon SNS notification for violations.
B. Use IAM CloudTrail to make a trail, and apply it to all Regions Specify an Amazon S3 bucket to receive all the CloudTrail log files
C. Add the following bucket policy to the company's IAM CloudTrail bucket to prevent log tampering{"Version": "2012-10-17-,"Statement": { "Effect":
"Deny","Action": "s3:PutObject", "Principal": "-","Resource": "arn:IAM:s3:::cloudtrail/IAMLogs/111122223333/*"}}Create an Amazon S3 data event for an PutObject attempts, which sends notifications to an Amazon SNS topic.
D. Create a Security Auditor role with permissions to access Amazon CloudWatch Logs m all Regions Ship the logs to an Amazon S3 bucket and make a lifecycle policy to ship the logs to Amazon S3 Glacier.
E. Verify that Amazon GuardDuty is enabled in all Regions, and create an Amazon CloudWatch Events rule for Amazon GuardDuty findings Add an Amazon SNS topic as the rule's target

**Answer:** AE

**NEW QUESTION 94**
A company is designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS Single Sign-On (AWS SSO). The company must implement a solution so that the development teams can use only specific AWS Regions and so that each AWS account allows access to only specific AWS services.
Which solution will meet these requirements with the LEAST operational overhead?

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

**Answer:** C

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

**NEW QUESTION 95**
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 97**
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 100**
A company uses AWS Organizations to manage a multi-accountAWS environment in a single AWS Region. The organization's management account is named management-01. The company has turned on AWS Config in all accounts in the organization. The company has designated an account named security-01 as the delegated administra-tor for AWS Config.
All accounts report the compliance status of each account's rules to the AWS Config delegated administrator account by using an AWS Config aggregator. Each account administrator can configure and manage the account's own AWS Config rules to handle each account's unique compliance requirements.
A security engineer needs to implement a solution to automatically deploy a set of 10 AWS Config rules to all existing and future AWS accounts in the organiza-tion. The solution must turn on AWS Config automatically during account crea-tion.
Which combination of steps will meet these requirements? (Select TWO.)

A. Create an AWS CloudFormation template that contains the 1 0 required AVVS Config rule
B. Deploy the template by using CloudFormation StackSets in the security-01 account.
C. Create a conformance pack that contains the 10 required AWS Config rule
D. Deploy the conformance pack from the security-01 account.
E. Create a conformance pack that contains the 10 required AWS Config rule
F. Deploy the conformance pack from the management-01 account.
G. Create an AWS CloudFormation template that will activate AWS Confi
H. De-ploy the template by using CloudFormation StackSets in the security-01 ac-count.
I. Create an AWS CloudFormation template that will activate AWS Confi
J. De-ploy the template by using CloudFormation StackSets in the management-01 account.

**Answer:** BE


**NEW QUESTION 105**
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 108**
A company used a lift-and-shift approach to migrate from its on-premises data centers to the AWS Cloud. The company migrated on-premises VMS to Amazon EC2 in-stances. Now the company wants to replace some of components that are running on the EC2 instances with managed AWS services that provide similar functionality.
Initially, the company will transition from load balancer software that runs on EC2 instances to AWS Elastic Load Balancers. A security engineer must ensure that after this transition, all the load balancer logs are centralized and searchable for auditing. The security engineer must also ensure that metrics are generated to show which ciphers are in use.

Which solution will meet these requirements?

A. Create an Amazon CloudWatch Logs log grou
B. Configure the load balancers to send logs to the log grou
C. Use the CloudWatch Logs console to search the log
D. Create CloudWatch Logs filters on the logs for the required met-rics.
E. Create an Amazon S3 bucke
F. Configure the load balancers to send logs to the S3 bucke
G. Use Amazon Athena to search the logs that are in the S3 bucke
H. Create Amazon CloudWatch filters on the S3 log files for the re-quired metrics.
I. Create an Amazon S3 bucke
J. Configure the load balancers to send logs to the S3 bucke
K. Use Amazon Athena to search the logs that are in the S3 bucke
L. Create Athena queries for the required metric
M. Publish the metrics to Amazon CloudWatch.
N. Create an Amazon CloudWatch Logs log grou
O. Configure the load balancers to send logs to the log grou
P. Use the AWS Management Console to search the log
Q. Create Amazon Athena queries for the required metric
R. Publish the metrics to Amazon CloudWatch.

**Answer:** C

**Explanation:**

≫ Amazon S3 is a service that provides scalable, durable, and secure object storage. You can use Amazon S3 to store and retrieve any amount of data from anywhere on the web1

≫ AWS Elastic Load Balancing is a service that distributes incoming application or network traffic across multiple targets, such as EC2 instances, containers, or IP addresses. You can use Elastic Load Balancing to increase the availability and fault tolerance of your applications2

≫ Elastic Load Balancing supports access logging, which captures detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use access logs to analyze traffic patterns and troubleshoot issues3

≫ You can configure your load balancer to store access logs in an Amazon S3 bucket that you specify.
You can also specify the interval for publishing the logs, which can be 5 or 60 minutes. The logs are stored in a hierarchical folder structure by load balancer name, IP address, year, month, day, and time.

≫ Amazon Athena is a service that allows you to analyze data in Amazon S3 using standard SQL. You can use Athena to run ad-hoc queries and get results in seconds. Athena is serverless, so there is no infrastructure to manage and you pay only for the queries that you run.

≫ You can use Athena to search the access logs that are stored in your S3 bucket. You can create a table in Athena that maps to your S3 bucket and then run SQL queries on the table. You can also use the Athena console or API to view and download the query results.

≫ You can also use Athena to create queries for the required metrics, such as the number of requests per cipher or protocol. You can then publish the metrics to Amazon CloudWatch, which is a service that monitors and manages your AWS resources and applications. You can use CloudWatch to collect and track metrics, create alarms, and automate actions based on the state of your resources.

≫ By using this solution, you can meet the requirements of ensuring that all the load balancer logs are centralized and searchable for auditing and that metrics are generated to show which ciphers are in use.

**NEW QUESTION 110**
A security engineer is configuring a mechanism to send an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. The security engineer creates a trail in AWS CloudTrail to assist in this work.
Which solution will meet these requirements?

A. In CloudTrail, turn on Insights events on the trai
B. Configure an alarm on the insight with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Configure a threshold of 3 and a period of 5 minutes.
C. Configure CloudTrail to send events to Amazon CloudWatch Log
D. Create a metric filter for the relevant log grou
E. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.
F. Create an Amazon Athena table from the CloudTrail event
G. Run a query for eventName matching ConsoleLogin and for errorMessage matching "Failed authentication". Create a notification action from the query to send an Amazon Simple Notification Service (Amazon SNS) notification when the count equals 3 within a period of 5 minutes.
H. In AWS Identity and Access Management Access Analyzer, create a new analyze
I. Configure the analyzer to send an Amazon Simple Notification Service (Amazon SNS) notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes.

**Answer:** B

**Explanation:**
The correct answer is B. Configure CloudTrail to send events to Amazon CloudWatch Logs. Create a metric filter for the relevant log group. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.
This answer is correct because it meets the requirements of sending an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. By configuring CloudTrail to send events to CloudWatch Logs, the security engineer can create a metric filter that matches the desired pattern of failed sign-in events. Then, by creating a CloudWatch alarm based on the metric filter, the security engineer can set a threshold of 3 and a period of 5 minutes, and choose an action such as sending an email or an Amazon Simple Notification Service (Amazon SNS) message when the alarm is triggered12.
The other options are incorrect because:

≫ A. Turning on Insights events on the trail and configuring an alarm on the insight is not a solution, because Insights events are used to analyze unusual activity in management events, such as spikes in API call volume or error rates. Insights events do not capture failed sign-in attempts to the AWS Management Console3.

≫ C. Creating an Amazon Athena table from the CloudTrail events and running a query for failed sign-in events is not a solution, because it does not provide a mechanism to send an alert based on the query results. Amazon Athena is an interactive query service that allows analyzing data in Amazon S3 using standard

SQL, but it does not support creating notifications or alarms from queries4.

D. Creating an analyzer in AWS Identity and Access Management Access Analyzer and configuring it to send an Amazon SNS notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes is not a solution, because IAM Access Analyzer is not a service that monitors sign-in events, but a service that helps identify resources that are shared with external entities. IAM Access Analyzer does not generate findings for failed sign-in attempts to the AWS Management Console5.

References:

1: Sending CloudTrail Events to CloudWatch Logs - AWS CloudTrail 2: Creating Alarms Based on Metric Filters - Amazon CloudWatch 3: Analyzing unusual activity in management events - AWS CloudTrail 4: What is Amazon Athena? - Amazon Athena 5: Using AWS Identity and Access Management Access Analyzer - AWS Identity and Access Management

## NEW QUESTION 111

An international company wants to combine AWS Security Hub findings across all the company's AWS Regions and from multiple accounts. In addition, the company
wants to create a centralized custom dashboard to correlate these findings with operational data for deeper
analysis and insights. The company needs an analytics tool to search and visualize Security Hub findings. Which combination of steps will meet these requirements? (Select THREE.)

A. Designate an AWS account as a delegated administrator for Security Hu
B. Publish events to Amazon CloudWatch from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.
C. Designate an AWS account in an organization in AWS Organizations as a delegated administrator for Security Hu
D. Publish events to Amazon EventBridge from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.
E. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis data strea
F. Configure the Kinesis data streams to output the logs to a single Amazon S3 bucket.
G. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery strea
H. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket.
I. Use AWS Glue DataBrew to crawl the Amazon S3 bucket and build the schem
J. Use AWS Glue Data Catalog to query the data and create views to flatten nested attribute
K. Build Amazon QuickSight dashboards by using Amazon Athena.
L. Partition the Amazon S3 dat
M. Use AWS Glue to crawl the S3 bucket and build the schem
N. Use Amazon Athena to query the data and create views to flatten nested attribute
O. Build Amazon QuickSight dashboards that use the Athena views.

**Answer:** BDF

**Explanation:**
The correct answer is B, D, and F. Designate an AWS account in an organization in AWS Organizations as a delegated administrator for Security Hub. Publish events to Amazon EventBridge from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery stream. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket. Partition the Amazon S3 data. Use AWS Glue to crawl the S3 bucket and build the schema. Use Amazon Athena to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards that use the Athena views.
According to the AWS documentation, AWS Security Hub is a service that provides you with a comprehensive view of your security state across your AWS accounts, and helps you check your environment against security standards and best practices. You can use Security Hub to aggregate security findings from various sources, such as AWS services, partner products, or your own applications.
To use Security Hub with multiple AWS accounts and Regions, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use Security Hub as a service principal for AWS Organizations, which lets you designate a delegated administrator account for Security Hub. The delegated administrator account can enable Security Hub automatically in all existing and future accounts in your organization, and can view and manage findings from all accounts.
According to the AWS documentation, Amazon EventBridge is a serverless event bus that makes it easy to connect applications using data from your own applications, integrated software as a service (SaaS) applications, and AWS services. You can use EventBridge to create rules that match events from various sources and route them to targets for processing.
To use EventBridge with Security Hub findings, you need to enable Security Hub as an event source in EventBridge. This will allow you to publish events from Security Hub to EventBridge in the same Region. You can then create EventBridge rules that match Security Hub findings based on criteria such as severity, type, or resource. You can also specify targets for your rules, such as Lambda functions, SNS topics, or Kinesis Data Firehose delivery streams.
According to the AWS documentation, Amazon Kinesis Data Firehose is a fully managed service that delivers real-time streaming data to destinations such as Amazon S3, Amazon Redshift, Amazon Elasticsearch Service (Amazon ES), and Splunk. You can use Kinesis Data Firehose to transform and enrich your data before delivering it to your destination.
To use Kinesis Data Firehose with Security Hub findings, you need to create a Kinesis Data Firehose delivery stream in each Region where you have enabled Security Hub. You can then configure the delivery stream to receive events from EventBridge as a source, and deliver the logs to a single S3 bucket as a destination. You can also enable data transformation or compression on the delivery stream if needed.
According to the AWS documentation, Amazon S3 is an object storage service that offers scalability, data availability, security, and performance. You can use S3 to store and retrieve any amount of data from anywhere on the web. You can also use S3 features such as lifecycle management, encryption, versioning, and replication to optimize your storage.
To use S3 with Security Hub findings, you need to create an S3 bucket that will store the logs from Kinesis Data Firehose delivery streams. You can then partition the data in the bucket by using prefixes such as account ID or Region. This will improve the performance and cost-effectiveness of querying the data.
According to the AWS documentation, AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load your data for analytics. You can use Glue to crawl your data sources, identify data formats, and suggest schemas and transformations. You can also use Glue Data Catalog as a central metadata repository for your data assets.
To use Glue with Security Hub findings, you need to create a Glue crawler that will crawl the S3 bucket and build the schema for the data. The crawler will create tables in the Glue Data Catalog that you can query using standard SQL.
According to the AWS documentation, Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. You can use Athena with Glue Data Catalog as a metadata store for your tables.
To use Athena with Security Hub findings, you need to create views in Athena that will flatten nested attributes in the data. For example, you can create views that extract fields such as account ID, Region, resource type, resource ID, finding type, finding title, and finding description from the JSON data. You can then query the views using SQL and join them with other tables if needed.
According to the AWS documentation, Amazon QuickSight is a fast, cloud-powered business intelligence
service that makes it easy to deliver insights to everyone in your organization. You can use QuickSight to create and publish interactive dashboards that include machine learning insights. You can also use QuickSight to connect to various data sources, such as Athena, S3, or RDS.

To use QuickSight with Security Hub findings, you need to create QuickSight dashboards that use the Athena views as data sources. You can then visualize and analyze the findings using charts, graphs, maps, or tables. You can also apply filters, calculations, or aggregations to the data. You can then share the dashboards with your users or embed them in your applications.

**NEW QUESTION 114**
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 116**
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 119**
A security team is working on a solution that will use Amazon EventBridge (Amazon CloudWatch Events) to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.
Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event. However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.
The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.
Which solution will meet these requirements?

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

**Answer:** D

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

> A. Modifying the EventBridge event pattern by selecting Amazon S3 and All Events as the event type will not capture the s3:PutObjectAcl API call, because this is a data event and not a management event. Management events provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations4.

> B. Modifying the EventBridge event pattern by selecting Amazon S3 and Bucket Level Operations as the event type will not capture the s3:PutObjectAcl API call, because this is a data event that affects the S3 object resource type and not the S3 bucket resource type. Bucket level operations are management events that affect the configuration or metadata of an S3 bucket5.

> C. Enabling CloudTrail Insights to identify unusual API activity will not help the security team monitor new S3 objects or changes to any S3 bucket policy or setting that result in public access. CloudTrail Insights helps AWS users identify and respond to unusual activity associated with API calls and API error rates by

continuously analyzing CloudTrail management events6. It does not analyze data events or generate EventBridge events.
References:
1: CloudTrail log event reference - AWS CloudTrail 2: Logging data events - AWS CloudTrail 3: PutObjectAcl - Amazon Simple Storage Service 4: [Logging management events - AWS CloudTrail] 5: [Amazon S3 Event Types - Amazon Simple Storage Service] 6: Logging Insights events for trails - AWS CloudTrail

**NEW QUESTION 120**
A developer is building a serverless application hosted on AWS that uses Amazon Redshift as a data store The application has separate modules for readwrite and read-only functionality The modules need their own database users for compliance reasons
Which combination of steps should a security engineer implement to grant appropriate access? (Select TWO.)

A. Configure cluster security groups for each application module to control access to database users that are required for read-only and readwrite
B. Configure a VPC endpoint for Amazon Redshift Configure an endpoint policy that maps database users to each application module, and allow access to the tables that are required for read-only and read/write
C. Configure an 1AM policy for each module Specify the ARN of an Amazon Redshift database user that allows the GetClusterCredentials API call
D. Create local database users for each module
E. Configure an 1AM policy for each module Specify the ARN of an 1AM user that allows the GetClusterCredentials API call

**Answer:** A

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

**NEW QUESTION 123**
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 124**
A company Is planning to use Amazon Elastic File System (Amazon EFS) with its on-premises servers. The company has an existing IAM Direct Connect connection established between its on-premises data center and an IAM Region Security policy states that the company's on-premises firewall should only have specific IP addresses added to the allow list and not a CIDR range. The company also wants to restrict access so that only certain data center-based servers have access to Amazon EFS
How should a security engineer implement this solution"

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

**Answer:** B

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

➤ Assign an Elastic IP address to Amazon EFS and add the Elastic IP address to the allow list for the data center firewall. This allows the security engineer to use a specific IP address for the EFS file system that can be added to the firewall rules, instead of a CIDR range or a URL.

➤ Install the AWS CLI on the data center-based servers to mount the EFS file system. This allows the security engineer to use the mount helper provided by AWS CLI to mount the EFS file system with encryption in transit.

➤ In the EFS security group, add the IP addresses of the data center servers to the allow list. This allows the security engineer to restrict access to the EFS file system to only certain data center-based servers.

➤ Mount the EFS using the Elastic IP address. This allows the security engineer to use the Elastic IP address as the DNS name for mounting the EFS file system.

**NEW QUESTION 129**
A company has multiple departments. Each department has its own IAM account. All these accounts belong to the same organization in IAM Organizations.
A large .csv file is stored in an Amazon S3 bucket in the sales department's IAM account. The company wants to allow users from the other accounts to access the

.csv file's content through the combination of IAM Glue and Amazon Athena. However, the company does not want to allow users from the other accounts to access other files in the same folder.
Which solution will meet these requirements?

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

**Answer:** A


**NEW QUESTION 131**
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 132**
......

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons and Answers in PDF Format

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

* AWS-Certified-Security-Specialty Questions and Answers Updated Frequently

* AWS-Certified-Security-Specialty Practice Questions Verified by Expert Senior Certified Staff

* AWS-Certified-Security-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AWS-Certified-Security-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

## 100% Actual & Verified — Instant Download, Please Click
Order The AWS-Certified-Security-Specialty Practice Test Here