Amazon-Web-Services

Exam Questions SCS-C02

AWS Certified Security - Specialty

NEW QUESTION 1
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 2
A company is using an AWS Key Management Service (AWS KMS) AWS owned key in its application to encrypt files in an AWS account The company's security team wants the ability to change to new key material for new files whenever a potential key breach occurs A security engineer must implement a solution that gives the security team the ability to change the key whenever the team wants to do so
Which solution will meet these requirements?

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

Answer: A

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

NEW QUESTION 3
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 4
A company has several workloads running on AWS. Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the Security Engineer implement employee-only access to this system without changing the application?

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

Answer: A

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

NEW QUESTION 5
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 6
A security engineer needs to build a solution to turn IAM CloudTrail back on in multiple IAM Regions in case it is ever turned off.
What is the MOST efficient way to implement this solution?

A. Use IAM Config with a managed rule to trigger the IAM-EnableCloudTrail remediation.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) event with a cloudtrail.amazonIAM.com event source and a StartLogging event name to trigger an IAM Lambda function to call the StartLogging API.
C. Create an Amazon CloudWatch alarm with a cloudtrail.amazonIAM.com event source and a StopLogging event name to trigger an IAM Lambda function to call the StartLogging API.
D. Monitor IAM Trusted Advisor to ensure CloudTrail logging is enabled.

Answer: B

NEW QUESTION 7
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 8
Your CTO thinks your IAM account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated IAM engineers and doing everything they can to cover their tracks?
Please select:

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

Answer: A

Explanation:
The IAM Documentation mentions the following
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. You can use the IAM CLI to validate the files in the location where CloudTrail delivered them
Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.
Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs For more information on Cloudtrail log file validation, please visit the below URL: http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html
The correct answer is: Use CloudTrail Log File Integrity Validation. omit your Feedback/Queries to our Expert

NEW QUESTION 9
A company uses an external identity provider to allow federation into different IAM accounts. A security engineer for the company needs to identify the federated user that terminated a production Amazon EC2 instance a week ago.
What is the FASTEST way for the security engineer to identify the federated user?

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

Answer: B

Explanation:
The fastest way to identify the federated user who terminated a production Amazon EC2 instance is to filter the IAM CloudTrail event history for the TerminateInstances event and identify the assumed IAM role. Then, review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username. This method does not require any additional tools or queries, and it directly links the IAM role with the federated user.
Option A is incorrect because the role session name may not be the same as the federated user name, and it may not be unique or descriptive enough to identify the user.
Option C is incorrect because the IAM Access Advisor tab only shows when a role was last accessed, not by whom or for what purpose. It also does not show the specific time of access, only the date.
Option D is incorrect because using Amazon Athena to run SQL queries on the IAM CloudTrail logs is not the fastest way to identify the federated user, as it requires creating a table schema and running multiple queries. It also assumes that the federation is done using web identity providers, not SAML providers, as indicated by the AssumeRoleWithWebIdentity event.
References:

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

NEW QUESTION 10
A security engineer is checking an AWS CloudFormation template for vulnerabilities. The security engineer finds a parameter that has a default value that exposes an application's API key in plaintext. The parameter is referenced several times throughout the template. The security engineer must replace the parameter while maintaining the ability to reference the value in the template. Which solution will meet these requirements in the MOST secure way? {resolve:s3:MyBucketName:MyObjectName}}.

A. Store the API key value as a SecureString parameter in AWS Systems Manager Parameter Stor
B. In the template, replace all references to the value with {{resolve:ssm:MySSMParameterName:I}}.
C. Store the API key value in AWS Secrets Manage

D. In the template, replace all references to the value with { {resolve:secretsmanager:MySecretId:SecretString}}.
E. Store the API key value in Amazon DynamoD
F. In the template, replace all references to the value with{{resolve:dynamodb:MyTableName:MyPrimaryKey}}.
G. Store the API key value in a new Amazon S3 bucke
H. In the template, replace all references to the value with {

Answer: B

Explanation:
The correct answer is B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with {{resolve:secretsmanager:MySecretId:SecretString}}.
This answer is correct because AWS Secrets Manager is a service that helps you protect secrets that are needed to access your applications, services, and IT resources. You can store and manage secrets such as database credentials, API keys, and other sensitive data in Secrets Manager. You can also use Secrets Manager to rotate, manage, and retrieve your secrets throughout their lifecycle1. Secrets Manager integrates with AWS CloudFormation, which allows you to reference secrets from your templates using the
{{resolve:secretsmanager:…}} syntax2. This way, you can avoid exposing your secrets in plaintext and still
use them in your resources.
The other options are incorrect because:

- A. Storing the API key value as a SecureString parameter in AWS Systems Manager Parameter Store is not a solution, because AWS CloudFormation does not support references to SecureString parameters. This means that you cannot use the {{resolve:ssm:…}} syntax to retrieve encrypted parameter values from Parameter Store3. You would have to use a custom resource or a Lambda function to decrypt the parameter value, which adds complexity and overhead to your template.
- C. Storing the API key value in Amazon DynamoDB is not a solution, because AWS CloudFormation does not support references to DynamoDB items. This means that you cannot use the
{{resolve:dynamodb:…}} syntax to retrieve item values from DynamoDB tables4. You would have to use a custom resource or a Lambda function to query the DynamoDB table, which adds complexity and overhead to your template.
- D. Storing the API key value in a new Amazon S3 bucket is not a solution, because AWS CloudFormation does not support references to S3 objects. This means that you cannot use the
{{resolve:s3:…}} syntax to retrieve object values from S3 buckets5. You would have to use a custom resource or a Lambda function to download the object from S3, which adds complexity and overhead to your template.

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

NEW QUESTION 10
A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?

A. A customer managed CMK that uses customer provided key material
B. A customer managed CMK that uses AWS provided key material
C. An AWS managed CMK
D. Operation system-native encryption that uses GnuPG

Answer: A

Explanation:
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/kms/import-key-material.html aws kms import-key-material \
--key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
--encrypted-key-material fileb://EncryptedKeyMaterial.bin \
--import-token fileb://ImportToken.bin \
--expiration-model KEY_MATERIAL_EXPIRES \
--valid-to 2021-09-21T19:00:00Z
The correct answer is A. A customer managed CMK that uses customer provided key material.
A customer managed CMK is a KMS key that you create, own, and manage in your AWS account. You have full control over the key configuration, permissions, rotation, and deletion. You can use a customer managed CMK to encrypt and decrypt data in AWS services that are integrated with AWS KMS, such as Amazon EBS1.
A customer managed CMK can use either AWS provided key material or customer provided key material. AWS provided key material is generated by AWS KMS and never leaves the service unencrypted. Customer provided key material is generated outside of AWS KMS and imported into a customer managed CMK. You can specify an expiration date for the imported key material, after which the CMK becomes unusable until you reimport new key material2.
To meet the criteria of automatically expiring the key material in 90 days, you need to use customer provided key material and set the expiration date accordingly. This way, you can ensure that the data encrypted with the CMK will not be accessible after 90 days unless you reimport new key material and re-encrypt the data.
The other options are incorrect for the following reasons:
* B. A customer managed CMK that uses AWS provided key material does not expire automatically. You can enable automatic rotation of the key material every year, but this does not prevent access to the data encrypted with the previous key material. You would need to manually delete the CMK and its backing key material to make the data inaccessible3.
* C. An AWS managed CMK is a KMS key that is created, owned, and managed by an AWS service on your behalf. You have limited control over the key configuration, permissions, rotation, and deletion. You cannot use an AWS managed CMK to encrypt data in other AWS services or applications. You also cannot set an expiration date for the key material of an AWS managed CMK4.
* D. Operation system-native encryption that uses GnuPG is not a solution that uses AWS KMS. GnuPG is a command line tool that implements the OpenPGP standard for encrypting and signing data. It does not integrate with Amazon EBS or other AWS services. It also does not provide a way to automatically expire the key material used for encryption5.

References:
1: Customer Managed Keys - AWS Key Management Service 2: [Importing Key Material in AWS Key Management Service (AWS KMS) - AWS Key Management Service] 3: [Rotating Customer Master Keys - AWS Key Management Service] 4: [AWS Managed Keys - AWS Key Management Service] 5: The GNU Privacy Guard

NEW QUESTION 11
A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.

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

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

Answer: CE

Explanation:
AWS Secrets Manager is a service that helps you manage, retrieve, and rotate secrets such as database credentials, API keys, and other sensitive information. By configuring automatic rotation of credentials in AWS Secrets Manager, you can ensure that your secrets are changed regularly and securely, without requiring manual intervention or application downtime. You can also specify the rotation frequency and the rotation function that performs the logic of changing the credentials on the database and updating the secret in Secrets Manager1.
* E. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotated. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.
By configuring the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials, you can avoid hard-coding the credentials in your application code or configuration files. This way, your application can dynamically obtain the latest credentials from Secrets Manager whenever the password is rotated, without needing to restart or redeploy the application. To enable this, you need to grant permission to the instance role associated with the EC2 instance to access Secrets Manager using IAM policies2. You can also use the AWS SDK for Java to integrate your application with Secrets Manager3.

NEW QUESTION 15
A security engineer receives a notice from the AWS Abuse team about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS>-based storage The instance is making connections to known malicious addresses
The instance is in a development account within a VPC that is in the us-east-1 Region The VPC contains an internet gateway and has a subnet in us-east-1a and us-easMb Each subnet is associate with a route table that uses the internet gateway as a default route Each subnet also uses the default network ACL The suspicious EC2 instance runs within the us-east-1 b subnet. During an initial investigation a security engineer discovers that the suspicious instance is the only instance that runs in the subnet
Which response will immediately mitigate the attack and help investigate the root cause?

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

Answer: B

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

NEW QUESTION 20
A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM.
Which combination of IAM services and features will provide protection in this scenario? (Select THREE).

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

Answer: DEF

NEW QUESTION 21
A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.
What configuration is necessary to allow the virtual security appliance to route the traffic?

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

Answer: C

Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#eni-basics Source/destination checking "You must disable source/destination checks if the instance runs services such as network address translation, routing, or firewalls."
The correct answer is C. Disable the Network Source/Destination check on the security appliance's elastic network interface.
This answer is correct because disabling the Network Source/Destination check allows the virtual security appliance to route traffic that is not addressed to or from itself. By default, this check is enabled on all EC2 instances, and it prevents them from forwarding traffic that does not match their own IP or MAC addresses. However, for a virtual security appliance that acts as a router or a firewall, this check needs to be disabled, otherwise it will drop the traffic that it is supposed to route12.
The other options are incorrect because:

- A. Disabling network ACLs is not a solution, because network ACLs are optional layers of security for the subnets in a VPC. They can be used to allow or deny traffic based on IP addresses and ports, but they do not affect the routing behavior of the virtual security appliance3.
- B. Configuring the security appliance's elastic network interface for promiscuous mode is not a solution, because promiscuous mode is a mode for a network interface that causes it to pass all traffic it receives to the CPU, rather than passing only the frames that it is programmed to receive. Promiscuous mode is normally used for packet sniffing or monitoring, but it does not enable the network interface to route traffic4.
- D. Placing the security appliance in the public subnet with the internet gateway is not a solution, because it does not address the routing issue of the virtual security appliance. The security appliance can be placed in either a public or a private subnet, depending on the network design and security requirements, but it still needs to have the Network Source/Destination check disabled to route traffic properly5.

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

NEW QUESTION 22
A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.
How can a security engineer meet this requirement?

A. Create an HTTPS listener that uses a certificate that is managed by IAM Certificate Manager (ACM).
B. Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect toward secrecy (PFS).
C. Create an HTTPS listener that uses the Server Order Preference security feature.
D. Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).

Answer: A

NEW QUESTION 23
A business requires a forensic logging solution for hundreds of Docker-based apps running on Amazon EC2. The solution must analyze logs in real time, provide message replay, and persist logs.
Which Amazon Web Offerings (IAM) services should be employed to satisfy these requirements? (Select two.)

A. Amazon Athena
B. Amazon Kinesis
C. Amazon SQS
D. Amazon Elasticsearch
E. Amazon EMR

Answer: BD

NEW QUESTION 24
A company is using AWS Organizations to manage multiple accounts. The company needs to allow an IAM user to use a role to access resources that are in another organization's AWS account.
Which combination of steps must the company perform to meet this requirement? (Select TWO.)

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

Answer: BC

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

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

Verified References:

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

NEW QUESTION 26
The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.
What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

A. Use AWS Certificate Manager to encrypt all traffic between the client and application servers.
B. Review the application security groups to ensure that only the necessary ports are open.
C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
D. Use Amazon Inspector to periodically scan the backend instances.
E. Use AWS Key Management Services to encrypt all the traffic between the client and application servers.

Answer: BD

Explanation:
The steps that the Security Engineer should take to check for known vulnerabilities and limit the attack surface are:
- B. Review the application security groups to ensure that only the necessary ports are open. This is a good practice to reduce the exposure of the EC2 instances to potential attacks from the Internet. Application security groups are a feature of Azure that allow you to group virtual machines and define network security policies based on those groups1.
- D. Use Amazon Inspector to periodically scan the backend instances. This is a service that helps you to identify vulnerabilities and exposures in your EC2 instances and applications. Amazon Inspector can perform automated security assessments based on predefined or custom rules packages2.

NEW QUESTION 31
A company is using AWS Organizations to implement a multi-account strategy. The company does not have on-premises infrastructure. All workloads run on AWS. The company currently has eight member accounts. The company anticipates that it will have no more than 20 AWS accounts total at any time.
The company issues a new security policy that contains the following requirements:
• No AWS account should use a VPC within the AWS account for workloads.
• The company should use a centrally managed VPC that all AWS accounts can access to launch workloads in subnets.
• No AWS account should be able to modify another AWS account's application resources within the centrally managed VPC.
• The centrally managed VPC should reside in an existing AWS account that is named Account-A within an organization.
The company uses an AWS CloudFormation template to create a VPC that contains multiple subnets in Account-A. This template exports the subnet IDs through the CloudFormation Outputs section.
Which solution will complete the security setup to meet these requirements?

A. Use a CloudFormation template in the member accounts to launch workload
B. Configure the template to use the Fn::ImportValue function to obtain the subnet ID values.
C. Use a transit gateway in the VPC within Account-
D. Configure the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads.
E. Use AWS Resource Access Manager (AWS RAM) to share Account-A's VPC subnets with the remaining member account
F. Configure the member accounts to use the shared subnets to launch workloads.
G. Create a peering connection between Account-A and the remaining member account
H. Configure the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads.

Answer: C

Explanation:
The correct answer is C. Use AWS Resource Access Manager (AWS RAM) to share Account-A’s VPC
subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.
This answer is correct because AWS RAM is a service that helps you securely share your AWS resources across AWS accounts, within your organization or organizational units (OUs), and with IAM roles and users for supported resource types1. One of the supported resource types is VPC subnets2, which means you can share the subnets in Account-A’s VPC with the other member accounts using AWS RAM. This way, you can meet the requirements of using a centrally managed VPC, avoiding duplicate VPCs in each account, and launching workloads in shared subnets. You can also control the access to the shared subnets by using IAM policies and resource-based policies3, which can prevent one account from modifying another account’s resources.
The other options are incorrect because:
- A. Using a CloudFormation template in the member accounts to launch workloads and using the Fn::ImportValue function to obtain the subnet ID values is not a solution, because Fn::ImportValue can only import values that have been exported by another stack within the same region4. This means that you cannot use Fn::ImportValue to reference the subnet IDs that are exported by Account-A’s CloudFormation template, unless all the member accounts are in the same region as Account-A. This option also does not avoid creating duplicate VPCs in each account, which is one of the requirements.
- B. Using a transit gateway in the VPC within Account-A and configuring the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads is not a solution, because a transit gateway does not allow you to launch workloads in another account’s subnets. A transit gateway is a network transit hub that enables you to route traffic between your VPCs and on-premises networks5, but it does not enable you to share subnets across accounts.
- D. Creating a peering connection between Account-A and the remaining member accounts and configuring the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads is not a solution, because a VPC peering connection does not allow you to launch workloads in another account’s subnets. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately6, but it does not enable you to share subnets across accounts.

References:
1: What is AWS Resource Access Manager? 2: Shareable AWS resources 3: Managing permissions for shared resources 4: Fn::ImportValue 5: What is a transit gateway? 6: What is VPC peering?

NEW QUESTION 35
There is a requirement for a company to transfer large amounts of data between IAM and an on-premise location. There is an additional requirement for low latency and high consistency traffic to IAM. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below
Please select:

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

Answer: A

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

NEW QUESTION 37
A company has enabled Amazon GuardDuty in all AWS Regions as part of its security monitoring strategy. In one of its VPCs, the company hosts an Amazon EC2 instance that works as an FTP server. A high number of clients from multiple locations contact the FTP server. GuardDuty identifies this activity as a brute force attack because of the high number of connections that happen every hour.
The company has flagged the finding as a false positive, but GuardDuty continues to raise the issue. A security engineer must improve the signal-to-noise ratio without compromising the companys visibility of potential anomalous behavior.
Which solution will meet these requirements?

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

Answer: C

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

NEW QUESTION 38
A development team is using an IAM Key Management Service (IAM KMS) CMK to try to encrypt and decrypt a secure string parameter from IAM Systems Manager Parameter Store. However, the development team receives an error message on each attempt.
Which issues that are related to the CMK could be reasons for the error? (Select TWO.)

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

Answer: AD

NEW QUESTION 42
A developer at a company uses an SSH key to access multiple Amazon EC2 instances. The company discovers that the SSH key has been posted on a public GitHub repository. A security engineer verifies that the key has not been used recently.
How should the security engineer prevent unauthorized access to the EC2 instances?

A. Delete the key pair from the EC2 consol
B. Create a new key pair.
C. Use the ModifyInstanceAttribute API operation to change the key on any EC2 instance that is using the key.
D. Restrict SSH access in the security group to only known corporate IP addresses.
E. Update the key pair in any AMI that is used to launch the EC2 instance
F. Restart the EC2 instances.

Answer: C

Explanation:
To prevent unauthorized access to the EC2 instances, the security engineer should do the following:
> Restrict SSH access in the security group to only known corporate IP addresses. This allows the security engineer to use a virtual firewall that controls inbound and outbound traffic for their EC2 instances, and limit SSH access to only trusted sources.

NEW QUESTION 47
A business stores website images in an Amazon S3 bucket. The firm serves the photos to end users through Amazon CloudFront. The firm learned lately that the photographs are being accessible from nations in which it does not have a distribution license.
Which steps should the business take to safeguard the photographs and restrict their distribution? (Select two.)

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

Answer: AC

Explanation:
For Enable Geo-Restriction, choose Yes. For Restriction Type, choose Whitelist to allow access to certain countries, or choose Blacklist to block access from

certain countries. https://IAM.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/

NEW QUESTION 50
A company has a guideline that mandates the encryption of all Amazon S3 bucket data in transit. A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted.
Which S3 bucket policy will meet this requirement?

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

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

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

D. A screenshot of a computer code Description automatically generated

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

Answer: B

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

NEW QUESTION 54
A company has implemented IAM WAF and Amazon CloudFront for an application. The application runs on Amazon EC2 instances that are part of an Auto Scaling group. The Auto Scaling group is behind an Application Load Balancer (ALB).
The IAM WAF web ACL uses an IAM Managed Rules rule group and is associated with the CloudFront distribution. CloudFront receives the request from IAM WAF and then uses the ALB as the distribution's origin.
During a security review, a security engineer discovers that the infrastructure is susceptible to a large, layer 7 DDoS attack.
How can the security engineer improve the security at the edge of the solution to defend against this type of attack?

A. Configure the CloudFront distribution to use the Lambda@Edge featur
B. Create an IAM Lambda function that imposes a rate limit on CloudFront viewer request
C. Block the request if the rate limit is exceeded.
D. Configure the IAM WAF web ACL so that the web ACL has more capacity units to process all IAM WAF rules faster.
E. Configure IAM WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded.
F. Configure the CloudFront distribution to use IAM WAF as its origin instead of the ALB.

Answer: C

Explanation:
To improve the security at the edge of the solution to defend against a large, layer 7 DDoS attack, the security engineer should do the following:
> Configure AWS WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded. This allows the security engineer to use a rule that tracks the number of requests from a single IP address and blocks subsequent requests if they exceed a specified threshold within a specified time period.

NEW QUESTION 59
A Security Engineer has been tasked with enabling IAM Security Hub to monitor Amazon EC2 instances fix CVE in a single IAM account The Engineer has already enabled IAM Security Hub and Amazon Inspector m the IAM Management Console and has installed me Amazon Inspector agent on an EC2 instances that need to be monitored.
Which additional steps should the Security Engineer lake 10 meet this requirement?

A. Configure the Amazon inspector agent to use the CVE rule package
B. Configure the Amazon Inspector agent to use the CVE rule package Configure Security Hub to ingest from IAM inspector by writing a custom resource policy
C. Configure the Security Hub agent to use the CVE rule package Configure IAM Inspector lo ingest from Security Hub by writing a custom resource policy
D. Configure the Amazon Inspector agent to use the CVE rule package Install an additional Integration library Allow the Amazon Inspector agent to communicate with Security Hub

Answer: D

Explanation:
you need to configure the Amazon Inspector agent to use the CVE rule package, which is a set of rules that check for vulnerabilities and exposures on your EC2 instances5. You also need to install an additional integration library that enables communication between the Amazon Inspector agent and Security Hub6. Security Hub is a service that provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices7. The other options are either incorrect or incomplete for meeting the requirement.

NEW QUESTION 62
A company that uses AWS Organizations is migrating workloads to AWS. The compa-nys application team determines that the workloads will use Amazon EC2 instanc-es, Amazon S3 buckets, Amazon DynamoDB tables, and Application Load Balancers. For each resource type, the company mandates that deployments must comply with the following requirements:
• All EC2 instances must be launched from approved AWS accounts.
• All DynamoDB tables must be provisioned with a standardized naming convention.
• All infrastructure that is provisioned in any accounts in the organization must be deployed by AWS CloudFormation templates.
Which combination of steps should the application team take to meet these re-quirements? (Select TWO.)

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

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

Answer: AD

NEW QUESTION 65
A company's security engineer wants to receive an email alert whenever Amazon GuardDuty, AWS Identity and Access Management Access Analyzer, or Amazon Made generate a high-severity security finding. The company uses AWS Control Tower to govern all of its accounts. The company also uses AWS Security Hub with all of the AWS service integrations turned on.
Which solution will meet these requirements with the LEAST operational overhead?

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

Answer: B

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

NEW QUESTION 70
A website currently runs on Amazon EC2, wan mostly statics content on the site. Recently the site was subjected to a DDoS attack a security engineer was (asked was redesigning the edge security to help
Mitigate this risk in the future.
What are some ways the engineer could achieve this (Select THREE)?

A. Use IAM X-Ray to inspect the trafc going to the EC2 instances.
B. Move the static content to Amazon S3, and front this with an Amazon Cloud Front distribution.
C. Change the security group conguration to block the source of the attack trafc
D. Use IAM WAF security rules to inspect the inbound trafc.
E. Use Amazon Inspector assessment templates to inspect the inbound traffic.
F. Use Amazon Route 53 to distribute trafc.

Answer: BDF

Explanation:
To redesign the edge security to help mitigate the DDoS attack risk in the future, the engineer could do the following:

- Move the static content to Amazon S3, and front this with an Amazon CloudFront distribution. This allows the engineer to use a global content delivery network that can cache static content at edge locations and reduce the load on the origin servers.
- Use AWS WAF security rules to inspect the inbound traffic. This allows the engineer to use web application firewall rules that can filter malicious requests based on IP addresses, headers, body, or URI strings, and block them before they reach the web servers.
- Use Amazon Route 53 to distribute traffic. This allows the engineer to use a scalable and highly available DNS service that can route traffic based on different policies, such as latency, geolocation, or health checks.

NEW QUESTION 71
A company wants to receive an email notification about critical findings in AWS Security Hub. The company does not have an existing architecture that supports this functionality.
Which solution will meet the requirement?

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

Answer: C

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

NEW QUESTION 76
A company wants to ensure that its IAM resources can be launched only in the us-east-1 and us-west-2 Regions.
What is the MOST operationally efficient solution that will prevent developers from launching Amazon EC2 instances in other Regions?

A. Enable Amazon GuardDuty in all Region
B. Create alerts to detect unauthorized activity outside us-east-1 and us-west-2.
C. Use an organization in IAM Organization
D. Attach an SCP that allows all actions when the IAM: Requested Region condition key is either us-east-1 or us-west-2. Delete the FullIAMAccess policy.
E. Provision EC2 resources by using IAM Cloud Formation templates through IAM CodePipelin
F. Allow only the values of us-east-1 and us-west-2 in the IAM CloudFormation template's parameters.
G. Create an IAM Config rule to prevent unauthorized activity outside us-east-1 and us-west-2.

Answer: C

NEW QUESTION 77
A company is testing its incident response plan for compromised credentials. The company runs a database on an Amazon EC2 instance and stores the sensitive data-base credentials as a secret in AWS Secrets Manager. The secret has rotation configured with an AWS Lambda function that uses the generic rotation function template. The EC2 instance and the Lambda function are deployed in the same pri-vate subnet. The VPC has a Secrets Manager VPC endpoint.
A security engineer discovers that the secret cannot rotate. The security engi-neer determines that the VPC endpoint is working as intended. The Amazon Cloud-Watch logs contain the following error:
"setSecret: Unable to log into database". Which solution will resolve this error?

A. Use the AWS Management Console to edit the JSON structure of the secret in Secrets Manager so that the secret automatically conforms with the struc-ture that the database requires.
B. Ensure that the security group that is attached to the Lambda function al-lows outbound connections to the EC2 instanc
C. Ensure that the security group that is attached to the EC2 instance allows inbound connections from the security group that is attached to the Lambda function.
D. Use the Secrets Manager list-secrets command in the AWS CLI to list the secre
E. Identify the database credential
F. Use the Secrets Manager rotate-secret command in the AWS CLI to force the immediate rotation of the se-cret.
G. Add an internet gateway to the VP
H. Create a NAT gateway in a public sub-ne
I. Update the VPC route tables so that traffic from the Lambda function and traffic from the EC2 instance can reach the Secrets Manager public endpoint.

Answer: B

Explanation:
This answer is correct because ensuring that the security groups allow bidirectional communication between the Lambda function and the EC2 instance will resolve the error. The error indicates that the Lambda function cannot connect to the database, which might be due to firewall rules blocking the traffic. By allowing outbound connections from the Lambda function and inbound connections to the EC2 instance, the security engineer can enable the rotation function to access and update the database credentials.

NEW QUESTION 80
A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross- account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

A. The external ID used by the Auditor is missing or incorrect.
B. The Auditor is using the incorrect password.
C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.
D. The Amazon EC2 role used by the Auditor must be set to the destination account role.
E. The secret key used by the Auditor is missing or incorrect.
F. The role ARN used by the Auditor is missing or incorrect.

Answer: ACF

Explanation:
The following may be causing the problem for the Auditor:
A. The external ID used by the Auditor is missing or incorrect. This is a possible cause, because the external ID is a unique identifier that is used to establish a trust relationship between the accounts. The external ID must match the one that is specified in the role's trust policy in the destination account1.
C. The Auditor has not been granted sts:AssumeRole for the role in the destination account. This is a possible cause, because sts:AssumeRole is the API action that allows the Auditor to assume the
cross-account role and obtain temporary credentials. The Auditor must have an IAM policy that allows them to call sts:AssumeRole for the role ARN in the destination account2.
F. The role ARN used by the Auditor is missing or incorrect. This is a possible cause, because the role ARN is the Amazon Resource Name of the cross-account role that the Auditor wants to assume. The role ARN must be valid and exist in the destination account3.

NEW QUESTION 85
A company is migrating one of its legacy systems from an on-premises data center to AWS. The application server will run on AWS, but the database must remain in the on-premises data center for compliance reasons. The database is sensitive to network latency. Additionally, the data that travels between the on-premises

data center and AWS must have IPsec encryption.
Which combination of AWS solutions will meet these requirements? (Choose two.)

A. AWS Site-to-Site VPN
B. AWS Direct Connect
C. AWS VPN CloudHub
D. VPC peering
E. NAT gateway

Answer: AB

Explanation:
The correct combination of AWS solutions that will meet these requirements is A. AWS Site-to-Site VPN and B. AWS Direct Connect.
* A. AWS Site-to-Site VPN is a service that allows you to securely connect your on-premises data center to your AWS VPC over the internet using IPsec encryption. This solution meets the requirement of encrypting the data in transit between the on-premises data center and AWS.
* B. AWS Direct Connect is a service that allows you to establish a dedicated network connection between your on-premises data center and your AWS VPC. This solution meets the requirement of reducing network latency between the on-premises data center and AWS.
* C. AWS VPN CloudHub is a service that allows you to connect multiple VPN connections from different locations to the same virtual private gateway in your AWS VPC. This solution is not relevant for this scenario, as there is only one on-premises data center involved.
* D. VPC peering is a service that allows you to connect two or more VPCs in the same or different regions using private IP addresses. This solution does not meet the requirement of connecting an on-premises data center to AWS, as it only works for VPCs.
* E. NAT gateway is a service that allows you to enable internet access for instances in a private subnet in your AWS VPC. This solution does not meet the requirement of connecting an on-premises data center to AWS, as it only works for outbound traffic from your VPC.

NEW QUESTION 89
A systems engineer deployed containers from several custom-built images that an application team provided through a QA workflow The systems engineer used Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type as the target platform The system engineer now needs to collect logs from all containers into an existing Amazon CloudWatch log group
Which solution will meet this requirement?

A. Turn on the awslogs log driver by specifying parameters for awslogs-group and awslogs-region m the LogConfiguration property
B. Download and configure the CloudWatch agent on the container instances
C. Set up Fluent Bit and FluentO as a DaemonSet to send logs to Amazon CloudWatch Logs
D. Configure an 1AM policy that includes the togs CreateLogGroup action Assign the policy to the container instances

Answer: A

Explanation:
The AWS documentation states that you can use the awslogs log driver to send log information to CloudWatch Logs. To use this method, you specify the parameters for awslogs-group and awslogs-region in the LogConfiguration property of the container definition. This method is the easiest way to send logs to CloudWatch Logs.
References: : Amazon Elastic Container Service Developer Guide

NEW QUESTION 93
A company needs complete encryption of the traffic between external users and an application. The company hosts the application on a fleet of Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB).
How can a security engineer meet these requirements?

A. Create a new Amazon-issued certificate in AWS Secrets Manage
B. Export the certificate from Secrets Manage
C. Import the certificate into the ALB and the EC2 instances.
D. Create a new Amazon-issued certificate in AWS Certificate Manager (ACM). Associate the certificate with the AL
E. Export the certificate from AC
F. Install the certificate on the EC2 instances.
G. Import a new third-party certificate into AWS Identity and Access Management (IAM). Export thecertificate from IA
H. Associate the certificate with the ALB and the EC2 instances.
I. Import a new third-party certificate into AWS Certificate Manager (ACM). Associate the certificate with the AL
J. Install the certificate on the EC2 instances.

Answer: D

Explanation:
The correct answer is D. Import a new third-party certificate into AWS Certificate Manager (ACM). Associate the certificate with the ALB. Install the certificate on the EC2 instances.
This answer is correct because it meets the requirements of complete encryption of the traffic between external users and the application. By importing a third-party certificate into ACM, the security engineer can use it to secure the communication between the ALB and the clients. By installing the same certificate on the EC2 instances, the security engineer can also secure the communication between the ALB and the instances. This way, both the front-end and back-end connections are encrypted with SSL/TLS1.
The other options are incorrect because:

- A. Creating a new Amazon-issued certificate in AWS Secrets Manager is not a solution, because AWS Secrets Manager is not a service for issuing certificates, but for storing and managing secrets such as database credentials and API keys2. AWS Secrets Manager does not integrate with ALB or EC2 for certificate deployment.
- B. Creating a new Amazon-issued certificate in AWS Certificate Manager (ACM) and exporting it from ACM is not a solution, because ACM does not allow exporting Amazon-issued certificates3. ACM only allows exporting private certificates that are issued by an AWS Private Certificate Authority (CA)4.
- C. Importing a new third-party certificate into AWS Identity and Access Management (IAM) is not a solution, because IAM is not a service for managing certificates, but for controlling access to AWS resources5. IAM does not integrate with ALB or EC2 for certificate deployment.

References:
1: How SSL/TLS works 2: What is AWS Secrets Manager? 3: Exporting an ACM Certificate 4: Exporting Private Certificates from ACM 5: What is IAM?

NEW QUESTION 97
Your company uses IAM to host its resources. They have the following requirements
1) Record all API calls and Transitions
2) Help in understanding what resources are there in the account
3) Facility to allow auditing credentials and logins
Which services would suffice the above requirements Please select:

A. IAM Inspector, CloudTrail, IAM Credential Reports
B. CloudTrai
C. IAM Credential Reports, IAM SNS
D. CloudTrail, IAM Config, IAM Credential Reports
E. IAM SQS, IAM Credential Reports, CloudTrail

Answer: C

Explanation:
You can use IAM CloudTrail to get a history of IAM API calls and related events for your account. This history includes calls made with the IAM Management Console, IAM Command Line Interface, IAM SDKs, and other IAM services.
Options A,B and D are invalid because you need to ensure that you use the services of CloudTrail, IAM Config, IAM Credential Reports
For more information on Cloudtrail, please visit the below URL:
http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-user-guide.html
IAM Config is a service that enables you to assess, audit and evaluate the configurations of your IAM resources. Config continuously monitors and records your IAM resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between IAM resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, char management and operational troubleshooting.
For more information on the config service, please visit the below URL https://IAM.amazon.com/config/
You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the IAM Management Console, the IAM SDKs and Command Line Tools, or the IAM API.
For more information on Credentials Report, please visit the below URL: http://docs.IAM.amazon.com/IAM/latest/UserGuide/id credentials_getting-report.html
The correct answer is: CloudTrail, IAM Config, IAM Credential Reports Submit your Feedback/Queries to our Experts

NEW QUESTION 102
An ecommerce company has a web application architecture that runs primarily on containers. The application containers are deployed on Amazon Elastic Container Service (Amazon ECS). The container images for the application are stored in Amazon Elastic Container Registry (Amazon ECR).
The company's security team is performing an audit of components of the application architecture. The security team identifies issues with some container images that are stored in the container repositories.
The security team wants to address these issues by implementing continual scanning and on-push scanning of the container images. The security team needs to implement a solution that makes any findings from these scans visible in a centralized dashboard. The security team plans to use the dashboard to view these findings along with other security-related findings that they intend to generate in the future.
There are specific repositories that the security team needs to exclude from the scanning process. Which solution will meet these requirements?

A. Use Amazon Inspecto
B. Create inclusion rules in Amazon ECR to match repos-itories that need to be scanne
C. Push Amazon Inspector findings to AWS Se-curity Hub.
D. Use ECR basic scanning of container image
E. Create inclusion rules in Ama-zon ECR to match repositories that need to be scanne
F. Push findings to AWS Security Hub.
G. Use ECR basic scanning of container image
H. Create inclusion rules in Ama-zon ECR to match repositories that need to be scanne
I. Push findings to Amazon Inspector.
J. Use Amazon Inspecto
K. Create inclusion rules in Amazon Inspector to match repositories that need to be scanne
L. Push Amazon Inspector findings to AWS Config.

Answer: A

NEW QUESTION 106
A company is using AWS to run a long-running analysis process on data that is stored in Amazon S3 buckets. The process runs on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The EC2 instances are deployed in a private subnet Of a VPC that does not have internet access. The EC2 instances and the S3 buckets are in the same AWS account
The EC2 instances access the S3 buckets through an S3 gateway endpoint that has the default access policy. Each EC2 instance is associated With an instance profile role that has a policy that explicitly allows the s3:GetObject action and the s3:PutObject action for only the required S3 buckets.
The company learns that one or more of the EC2 instances are compromised and are exfiltrating data to an S3 bucket that is outside the companys organization in AWS Organizations. A security engtneer must implement a solution to stop this exfiltration of data and to keep the EC2 processing job functional.
Which solution will meet these requirements?

A. Update the policy on the S3 gateway endpoint to allow the S3 actions CY11y if the values of the aws:ResourceOrglD and aws:PrincipalOrglD condition keys match the companys values.
B. Update the policy on the instance profile role to allow the S3 actions only if the value of the aws:ResourceOrglD condition key matches the company's value.
C. Add a network ACL rule to the subnet of the EC2 instances to block outgoing connections on port 443.
D. Apply an SCP on the AWS account to allow the $3 actions only if the values of the aws:ResourceOrglD and aws:PrincipalOrglD condition keys match the company's values.

Answer: D

Explanation:
The correct answer is D.
To stop the data exfiltration from the compromised EC2 instances, the security engineer needs to implement a solution that can deny access to any S3 bucket that is outside the company’s organization. The solution should also allow the EC2 instances to access the required S3 buckets within the company’s organization for the analysis process.

Option A is incorrect because updating the policy on the S3 gateway endpoint will not affect the access to S3 buckets that are outside the company's organization. The S3 gateway endpoint only applies to S3 buckets that are in the same AWS Region as the VPC. The compromised EC2 instances can still access S3 buckets in other Regions or other AWS accounts through the internet gateway or NAT device.
Option B is incorrect because updating the policy on the instance profile role will not prevent the compromised EC2 instances from using other credentials or methods to access S3 buckets outside the company's organization. The instance profile role only applies to requests that are made using the credentials of that role. The compromised EC2 instances can still use other IAM users, roles, or access keys to access S3 buckets outside the company's organization.
Option C is incorrect because adding a network ACL rule to block outgoing connections on port 443 will also block legitimate connections to S3 buckets within the company's organization. The network ACL rule will prevent the EC2 instances from accessing any S3 bucket through HTTPS, regardless of whether it is inside or outside the company's organization.
Option D is correct because applying an SCP on the AWS account will effectively deny access to any S3 bucket that is outside the company's organization. The SCP will apply to all IAM users, roles, and resources in the AWS account, regardless of how they access S3. The SCP will use the aws:ResourceOrgID and aws:PrincipalOrgID condition keys to check whether the S3 bucket and the principal belong to the same organization as the AWS account. If they do not match, the SCP will deny the S3 actions.
References:

- Using service control policies
- AWS Organizations service control policy examples

NEW QUESTION 109
A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.
Which solution will meet these requirements MOST quickly?

A. Log in to the AWS account by using read-only credential
B. Review the GuardDuty finding for details about the IAM credentials that were use
C. Use the IAM console to add a DenyAll policy to the IAM principal.
D. Log in to the AWS account by using read-only credential
E. Review the GuardDuty finding to determine which API calls initiated the findin
F. Use Amazon Detective to review the API calls in context.
G. Log in to the AWS account by using administrator credential
H. Review the GuardDuty finding for details about the IAM credentials that were use
I. Use the IAM console to add a DenyAll policy to the IAM principal.
J. Log in to the AWS account by using read-only credential
K. Review the GuardDuty finding to determinewhich API calls initiated the findin
L. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

Answer: B

Explanation:
This answer is correct because logging in with read-only credentials minimizes the risk of accidental or malicious changes to the AWS account. Reviewing the GuardDuty finding can help identify which API calls initiated the finding and which IAM principal was involved. Using Amazon Detective can help analyze and visualize the API calls in context, such as which resources were affected, which IP addresses were used, and how the activity deviated from normal patterns. Amazon Detective can also help identify related findings from other sources, such as AWS Config or AWS Audit Manager.

NEW QUESTION 113
A company's on-premises networks are connected to VPCs using an IAM Direct Connect gateway. The company's on-premises application needs to stream data using an existing Amazon Kinesis Data Firehose delivery stream. The company's security policy requires that data be encrypted in transit using a private network.
How should the company meet these requirements?

A. Create a VPC endpoint tor Kinesis Data Firehos
B. Configure the application to connect to the VPC endpoint.
C. Configure an IAM policy to restrict access to Kinesis Data Firehose using a source IP condition.Configure the application to connect to the existing Firehose delivery stream.
D. Create a new TLS certificate in IAM Certificate Manager (ACM). Create a public-facing Network Load Balancer (NLB) and select the newly created TLS certificat
E. Configure the NLB to forward all traffic to Kinesis Data Firehos
F. Configure the application to connect to the NLB.
G. Peer the on-premises network with the Kinesis Data Firehose VPC using Direct Connec
H. Configure the application to connect to the existing Firehose delivery stream.

Answer: A

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

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

NEW QUESTION 116
A company uses infrastructure as code (IaC) to create AWS infrastructure. The company writes the code as AWS CloudFormation templates to deploy the infrastructure. The company has an existing CI/CD pipeline that the company can use to deploy these templates.
After a recent security audit, the company decides to adopt a policy-as-code approach to improve the company's security posture on AWS. The company must prevent the deployment of any infrastructure that would violate a security policy, such as an unencrypted Amazon Elastic Block Store (Amazon EBS) volume.
Which solution will meet these requirements?

A. Turn on AWS Trusted Adviso
B. Configure security notifications as webhooks in the preferences section of the CI/CD pipeline.

C. Turn on AWS Confi
D. Use the prebuilt rules or customized rule
E. Subscribe the CI/CD pipeline to anAmazon Simple Notification Service (Amazon SNS) topic that receives notifications from AWS Config.
F. Create rule sets in AWS CloudFormation Guar
G. Run validation checks for CloudFormation templates as a phase of the CI/CD process.
H. Create rule sets as SCP
I. Integrate the SCPs as a part of validation control in a phase of the CI/CD process.

Answer: C

Explanation:
The correct answer is C. Create rule sets in AWS CloudFormation Guard. Run validation checks for CloudFormation templates as a phase of the CI/CD process. This answer is correct because AWS CloudFormation Guard is a tool that helps you implement policy-as-code for your CloudFormation templates. You can use Guard to write rules that define your security policies, such as requiring encryption for EBS volumes, and then validate your templates against those rules before deploying them. You can integrate Guard into your CI/CD pipeline as a step that runs the validation checks and prevents the deployment of any non-compliant templates12.
The other options are incorrect because:

- A. Turning on AWS Trusted Advisor and configuring security notifications as webhooks in the preferences section of the CI/CD pipeline is not a solution, because AWS Trusted Advisor is not a policy-as-code tool, but a service that provides recommendations to help you follow AWS best practices. Trusted Advisor does not allow you to define your own security policies or validate your CloudFormation templates against them3.
- B. Turning on AWS Config and using the prebuilt or customized rules is not a solution, because AWS Config is not a policy-as-code tool, but a service that monitors and records the configuration changes of your AWS resources. AWS Config does not allow you to validate your CloudFormation templates before deploying them, but only evaluates the compliance of your resources after they are created4.
- D. Creating rule sets as SCPs and integrating them as a part of validation control in a phase of the CI/CD process is not a solution, because SCPs are not policy-as-code tools, but policies that you can use to manage permissions in your AWS Organizations. SCPs do not allow you to validate your CloudFormation templates, but only restrict the actions that users and roles can perform in your accounts5.

References:
1: What is AWS CloudFormation Guard? 2: Introducing AWS CloudFormation Guard 2.0 3: AWS Trusted Advisor 4: What Is AWS Config? 5: Service control policies - AWS Organizations

NEW QUESTION 120
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 122
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 123
A company's cloud operations team is responsible for building effective security for IAM cross-account access. The team asks a security engineer to help troubleshoot why some developers in the developer account (123456789012) in the developers group are not able to assume a cross-account role (ReadS3) into a production account (999999999999) to read the contents of an Amazon S3 bucket (productionapp). The two account policies are as follows:

Developer account 123456789012:
Developer group permissions:

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

Production account 999999999999:
Production account ReadS3 role policy:

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

Production account ReadS3 role policy - trust relationship:

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

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

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

Answer: AD

NEW QUESTION 124
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 127
A company has an organization in AWS Organizations that includes dedicated accounts for each of its business units. The company is collecting all AWS CloudTrail logs from the accounts in a single Amazon S3 bucket in the top-level account. The company's IT governance team has access to the top-level account.
A security engineer needs to allow each business unit to access its own CloudTrail logs.
The security engineer creates an IAM role in the top-level account for each of the other accounts. For each role the security engineer creates an IAM policy to allow read-only permissions to objects in the S3 bucket with the prefix of the respective logs.
Which action must the security engineer take in each business unit account to allow an IAM user in that account to read the logs?

A. Attach a policy to the IAM user to allow the user to assume the role that was created in the top-level accoun
B. Specify the role's ARN in the policy.
C. Create an SCP that grants permissions to the top-level account.
D. Use the root account of the business unit account to assume the role that was created in the top-level accoun
E. Specify the role's ARN in the policy.
F. Forward the credentials of the IAM role in the top-level account to the IAM user in the business unit account.

Answer: A

Explanation:
To allow an IAM user in one AWS account to access resources in another AWS account using IAM roles, the following steps are required:
- Create a role in the AWS account that contains the resources (the trusting account) and specify the AWS account that contains the IAM user (the trusted account) as a trusted entity in the role's trust policy. This allows users from the trusted account to assume the role and access resources in the trusting account.
- Attach a policy to the IAM user in the trusted account that allows the user to assume the role in the trusting account. The policy must specify the ARN of the role that was created in the trusting account.
- The IAM user can then switch roles or use temporary credentials to access the resources in the trusting account.

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

NEW QUESTION 132
A company has an AWS Lambda function that creates image thumbnails from larger images. The Lambda function needs read and write access to an Amazon S3 bucket in the same AWS account.
Which solutions will provide the Lambda function this access? (Select TWO.)

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

Answer: CD

NEW QUESTION 134
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": {
                "StringtEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

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

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

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

Answer: B

NEW QUESTION 138
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 140
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 142
A Security Engineer is asked to update an AWS CloudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the Security Engineer receives the following error message: `There is a problem with the bucket policy.` What will enable the Security Engineer to save the change?

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

Answer: C

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

A. Creating a new trail with the updated log file prefix, and then deleting the original trail is not necessary and may cause data loss or inconsistency. You can simply update the existing trail and its associated bucket policy with the new log file prefix.

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

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

References:

1: Using bucket policies - Amazon Simple Storage Service

NEW QUESTION 145

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 150

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

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

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

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

B)

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

C)

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

D)

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

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

Answer: A

NEW QUESTION 155
A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.
All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.
Which SCP should the security engineer attach to the root of the organization to meet these requirements?

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

B. A screenshot of a computer code Description automatically generated

C. A screenshot of a computer code Description automatically generated

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

D. A screenshot of a computer code Description automatically generated

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

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

Answer: A

NEW QUESTION 160
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 165

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SCS-C02 Practice Exam Features:

* SCS-C02 Questions and Answers Updated Frequently

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

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

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