Exam Questions SCS-C02

AWS Certified Security - Specialty

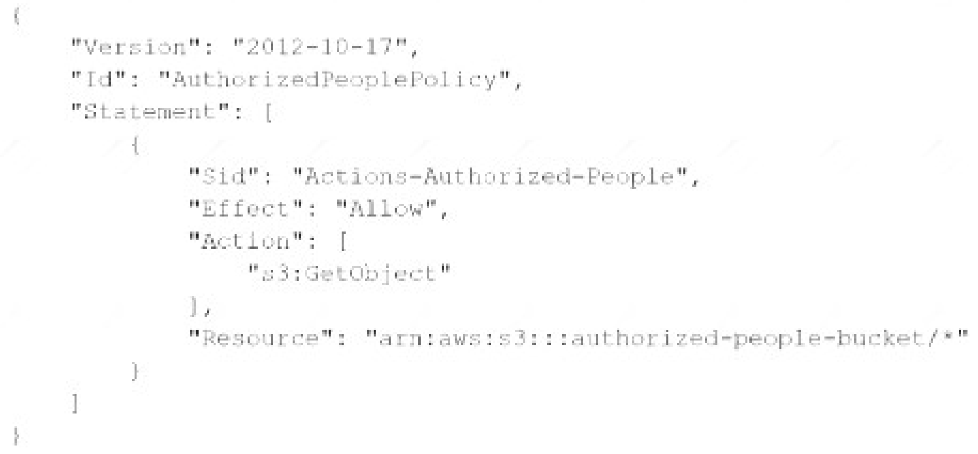
https://www.2passeasy.com/dumps/SCS-C02/

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.

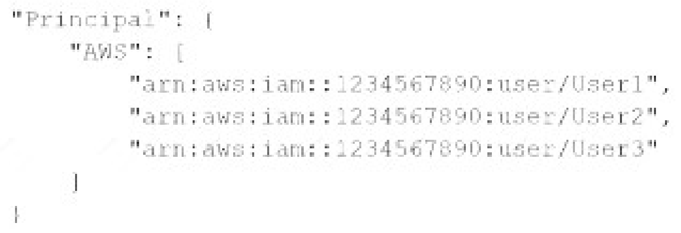
Answer: ACE

NEW QUESTION 2
A security engineer needs to create an Amazon S3 bucket policy to grant least privilege read access to IAM user accounts that are named User=1, User2. and User3. These IAM user accounts are members of the AuthorizedPeople IAM group. The security engineer drafts the following S3 bucket policy:



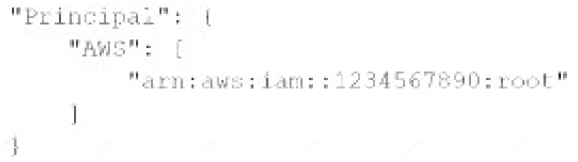
```
{
    "Version": "2012-10-17",
    "Id": "AuthorizedPeoplePolicy",
    "Statement": [
        {
            "Sid": "Actions-Authorized-People",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::authorized-people-bucket/*"
        }
    ]
}
```

When the security engineer tries to add the policy to the S3 bucket, the following error message appears: "Missing required field Principal." The security engineer is adding a Principal element to the policy. The addition must provide read access to only User1. User2, and User3. Which solution meets these requirements?
A)



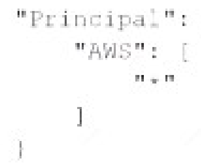
```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:user/User1",
        "arn:aws:iam::1234567890:user/User2",
        "arn:aws:iam::1234567890:user/User3"
    ]
}
```

B)



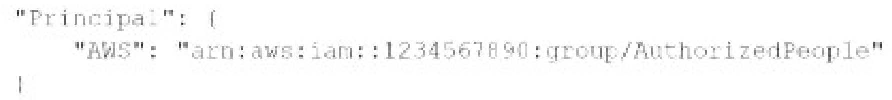
```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:root"
    ]
}
```

C)



```
"Principal": {
    "AWS": [
        "*"
    ]
}
```

D)



```
"Principal": {
    "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"
}
```

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

Answer: A

NEW QUESTION 3
A company's security team is building a solution for logging and visualization. The solution will assist the company with the large variety and velocity of data that it receives from IAM across multiple accounts. The security team has enabled IAM CloudTrail and VPC Flow Logs in all of its accounts. In addition, the company has an organization in IAM Organizations and has an IAM Security Hub master account.
The security team wants to use Amazon Detective However the security team cannot enable Detective and is unsure why
What must the security team do to enable Detective?

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

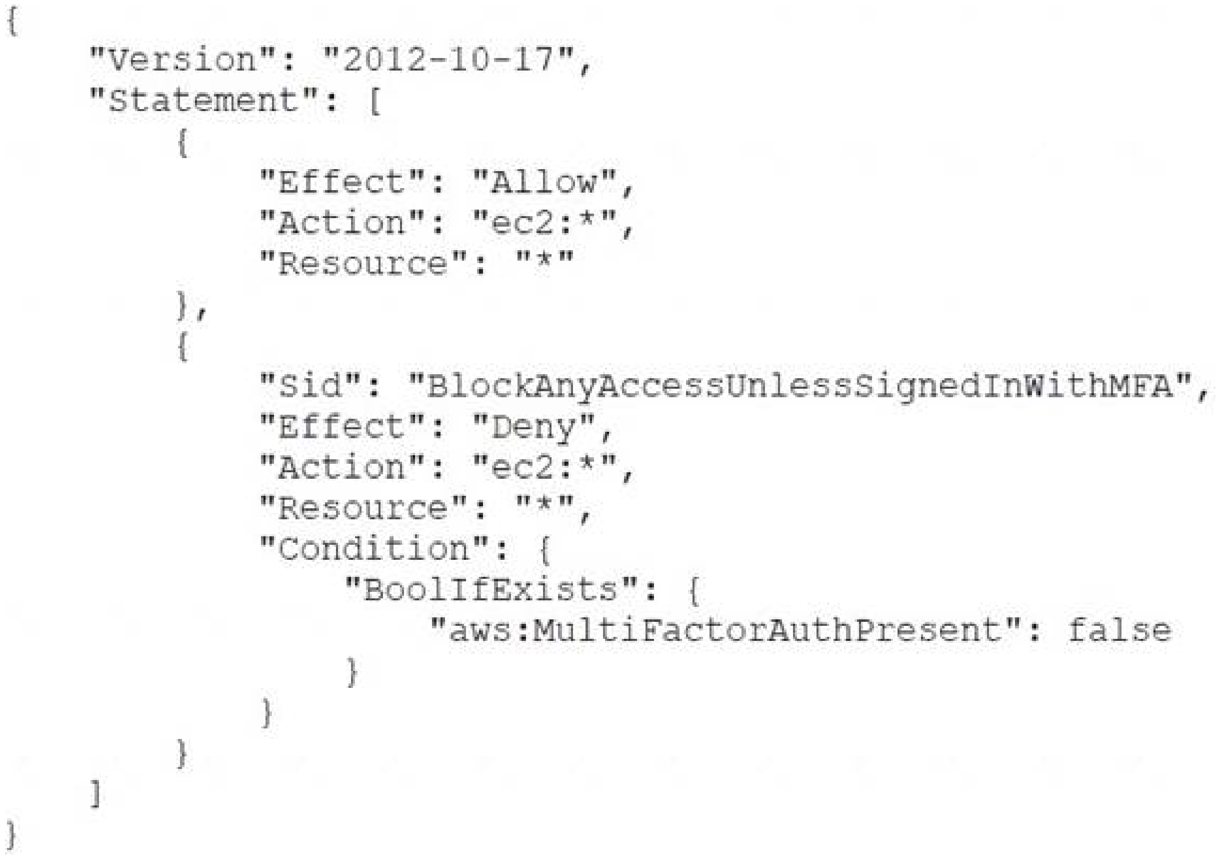
Answer: D

NEW QUESTION 4
A company developed an application by using AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS), and Amazon DynamoDB. An external application puts objects into the company's S3 bucket and tags the objects with date and time. A Lambda function periodically pulls data from the company's S3 bucket based on date and time tags and inserts specific values into a DynamoDB table for further processing.
The data includes personally identifiable information (Pll). The company must remove data that is older than 30 days from the S3 bucket and the DynamoDB table.
Which solution will meet this requirement with the MOST operational efficiency?

A. Update the Lambda function to add a TTL S3 flag to S3 object
B. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using the TTL S3 flag.
C. Create an S3 Lifecycle policy to expire objects that are older than 30 day
D. Update the Lambda function to add the TTL attribute in the DynamoDB tabl
E. Enable TTL on the DynamoDB table to expire entires that are older than 30 days based on the TTL attribute.
F. Create an S3 Lifecycle policy to expire objects that are older than 30 days and to add all prefixes to the S3 bucke
G. Update the Lambda function to delete entries that are older than 30 days.
H. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using object tag
I. Update the Lambda function to delete entries that are older than 30 days.

Answer: B

NEW QUESTION 5
An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:



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

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

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

Answer: B

Explanation:
The correct answer is B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication --serial-number and --token-code parameters. Use these resulting values to make API/CLI calls.
According to the AWS documentation1, the aws sts get-session-token CLI command returns a set of temporary credentials for an AWS account or IAM user. The credentials consist of an access key ID, a secret access key, and a security token. These credentials are valid for the specified duration only. The session duration for IAM users can be between 15 minutes and 36 hours, with a default of 12 hours.
You can use the --serial-number and --token-code parameters to provide the MFA device serial number and the MFA code from the device. The MFA device must be associated with the user who is making the
get-session-token call. If you do not provide these parameters when your IAM user or role has a policy that requires MFA, you will receive an Access Denied error.
The temporary security credentials that are returned by the get-session-token command can then be used to make subsequent API or CLI calls that require MFA authentication. You can use environment variables or a profile in your AWS CLI configuration file to specify the temporary credentials.
Therefore, this solution will resolve the problem of users being unable to perform EC2 commands using the AWS CLI, while still enforcing MFA.
The other options are incorrect because:

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

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

NEW QUESTION 6
A company is implementing new compliance requirements to meet customer needs. According to the new requirements the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster.
Which solution will meet these requirements in the MOST operationally efficient manner?

A. Create an AWS Config managed rule to detect unencrypted ROS storag
B. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
C. Configure the Lambda function to delete the unencrypted resource.
D. Create an AWS Config managed rule to detect unencrypted RDS storag
E. Configure a manual remediation action to invoke an AWS Lambda functio
F. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
G. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
H. Configure the Lambda function to delete the unencrypted resource.
I. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster
J. Configure the rule to invoke an AWS Lambda functio
K. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.

Answer: A

Explanation:
https://docs.aws.amazon.com/config/latest/developerguide/rds-storage-encrypted.html

NEW QUESTION 7
A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file. However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.
What should the security engineer do next to resolve the issue?

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

Answer: D

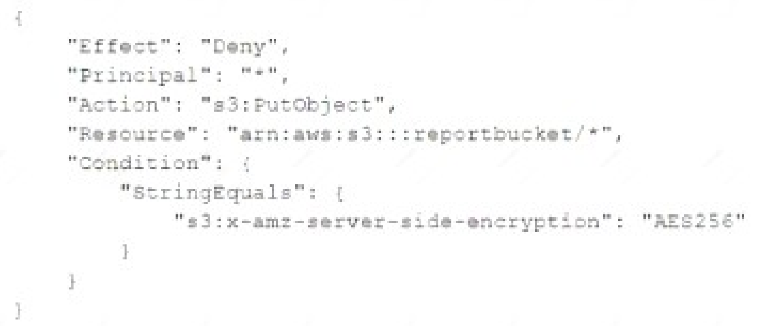
Explanation:
The correct answer is D. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.
According to the AWS documentation1, the CloudWatch agent is a software agent that you can install on your EC2 instances to collect system-level metrics and logs. To use the CloudWatch agent, you need to attach an IAM role or user to the EC2 instance that grants permissions for the agent to perform actions on your behalf. The CloudWatchAgentServerPolicy is an AWS managed policy that provides the necessary permissions for the agent to write metrics and logs to CloudWatch2. By attaching this policy to the EC2 instance role, the security engineer can resolve the issue of CloudWatch not receiving the custom application-security logs.
The other options are incorrect for the following reasons:

- A. Adding AWS CloudTrail to the trust policy of the EC2 instance is not relevant, because CloudTrail is a service that records API activity in your AWS account, not custom application logs3. Sending the custom logs to CloudTrail instead of CloudWatch would not meet the requirement of forwarding them to CloudWatch.
- B. Adding Amazon S3 to the trust policy of the EC2 instance is not necessary, because S3 is a storage service that does not require any trust relationship with

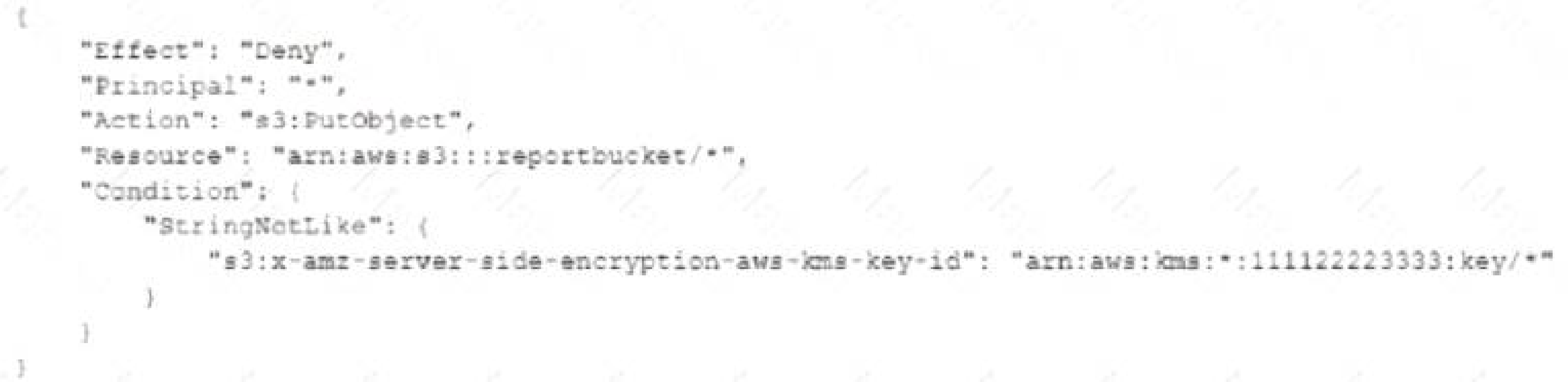
EC2 instances4. Configuring the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs would be an alternative solution, but it would be more complex and costly than using the CloudWatch agent directly.

> C. Adding Amazon Inspector to the trust policy of the EC2 instance is not helpful, because Inspector is a service that scans EC2 instances for software vulnerabilities and unintended network exposure, not custom application logs5. Using Amazon Inspector instead of the CloudWatch agent would not meet the requirement of forwarding them to CloudWatch.
References:
1: Collect metrics, logs, and traces with the CloudWatch agent - Amazon CloudWatch 2: CloudWatchAgentServerPolicy - AWS Managed Policy 3: What Is AWS CloudTrail? - AWS CloudTrail 4: Amazon S3 FAQs - Amazon Web Services 5: Automated Software Vulnerability Management - Amazon Inspector - AWS

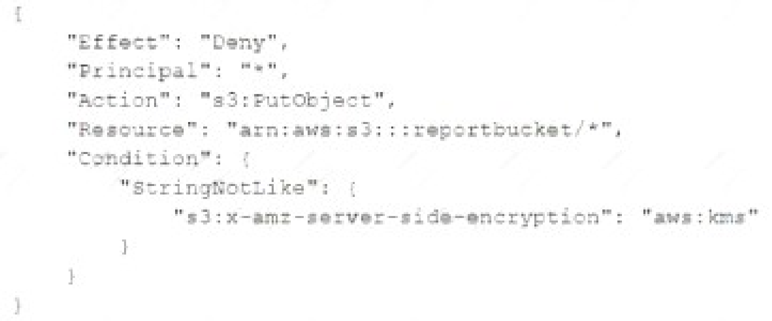
NEW QUESTION 8
A company uses an Amazon S3 bucket to store reports Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client-specified IAM Key Management Service (IAM KMS) CMK owned by the same account as the S3 bucket. The IAM account number is 111122223333, and the bucket name Is report bucket. The company's security specialist must write the S3 bucket policy to ensure the mandate can be Implemented
Which statement should the security specialist include in the policy?

A.


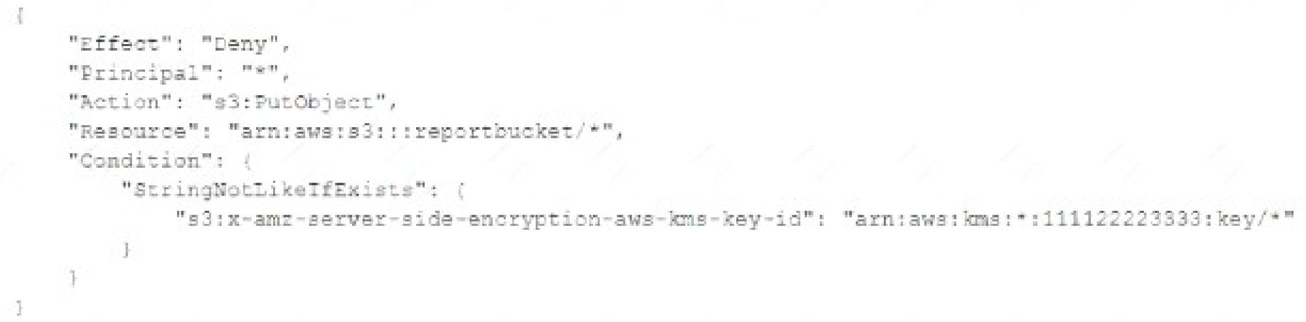
```
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::reportbucket/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-server-side-encryption": "AES256"
        }
    }
}
```

B.


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

C.


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

D.


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

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

Answer: D

NEW QUESTION 9
A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee. Even after updating the policy, the employee still receives an access denied message.
What is the likely cause of this access denial?

A. The ACL in the bucket needs to be updated
B. The IAM policy does not allow the user to access the bucket
C. It takes a few minutes for a bucket policy to take effect
D. The allow permission is being overridden by the deny

Answer: D

NEW QUESTION 10
A web application gives users the ability to log in verify their membership's validity and browse artifacts that are stored in an Amazon S3 bucket. When a user

attempts to download an object, the application must verify the permission to access the object and allow the user to download the object from a custom domain name such as example com.
What is the MOST secure way for a security engineer to implement this functionality?

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

Answer: D

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

NEW QUESTION 10
A company is building an application on AWS that will store sensitive information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.
What should the security engineer recommend?

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

Answer: C

NEW QUESTION 11
A company hosts business-critical applications on Amazon EC2 instances in a VPC. The VPC uses default DHCP options sets. A security engineer needs to log all DNS queries that internal resources make in the VPC. The security engineer also must create a list of the most common DNS queries over time.
Which solution will meet these requirements?

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

Answer: D

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

NEW QUESTION 13
A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company’s security policies for accessing other AWS resources from Amazon EC2.
A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLE-BUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.
The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).
Which combination of steps should the security engineer take to gather this information? (Choose two.)

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

Answer: AD

NEW QUESTION 18
A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.
The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.
Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

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

Answer: BCF

NEW QUESTION 20
A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot. What should the Security Engineer do to block the malicious bot?

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

Answer: D

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

NEW QUESTION 24
A security engineer is using AWS Organizations and wants to optimize SCPs. The security engineer needs to ensure that the SCPs conform to best practices.
Which approach should the security engineer take to meet this requirement?

A. Use AWS IAM Access Analyzer to analyze the policie
B. View the findings from policy validation checks.
C. Review AWS Trusted Advisor checks for all accounts in the organization.
D. Set up AWS Audit Manage
E. Run an assessment for all AWS Regions for all accounts.
F. Ensure that Amazon Inspector agents are installed on all Amazon EC2 in-stances in all accounts.

Answer: A

NEW QUESTION 29
A company that uses AWS Organizations wants to see AWS Security Hub findings for many AWS accounts and AWS Regions. Some of the accounts are in the company's organization, and some accounts are in organizations that the company manages for customers. Although the company can see findings in the Security Hub administrator account for accounts in the company's organization, there are no findings from accounts in other organizations.
Which combination of steps should the company take to see findings from accounts that are outside the organization that includes the Security Hub administrator account? (Select TWO.)

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

Answer: CE

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

- Send invitations to accounts that are outside the company's organization from the Security Hub administrator account. This will allow the administrator account to view and manage findings from those accounts. The administrator account can send invitations by using the Security Hub console, API, or CLI. For more information, see Sending invitations to member accounts.
- Send an administration request from the member accounts. This will allow the member accounts to accept the invitation from the administrator account and establish a relationship with it. The member accounts can send administration requests by using the Security Hub console, API, or CLI. For more information, see Sending administration requests.

This solution will enable the company to see Security Hub findings for many AWS accounts and AWS Regions, including accounts that are outside its own organization.
The other options are incorrect because they either do not establish a relationship between the administrator and member accounts (A, B), do not enable Security Hub for all member accounts (D), or do not use a valid service for Security Hub (F).
Verified References:

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

NEW QUESTION 34
An international company wants to combine AWS Security Hub findings across all the company's AWS Regions and from multiple accounts. In addition, the company
wants to create a centralized custom dashboard to correlate these findings with operational data for deeper
analysis and insights. The company needs an analytics tool to search and visualize Security Hub findings. Which combination of steps will meet these requirements? (Select THREE.)

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

Answer: BDF

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

According to the AWS documentation, Amazon QuickSight is a fast, cloud-powered business intelligence
service that makes it easy to deliver insights to everyone in your organization. You can use QuickSight to create and publish interactive dashboards that include machine learning insights. You can also use QuickSight to connect to various data sources, such as Athena, S3, or RDS.
To use QuickSight with Security Hub findings, you need to create QuickSight dashboards that use the Athena views as data sources. You can then visualize and analyze the findings using charts, graphs, maps, or tables. You can also apply filters, calculations, or aggregations to the data. You can then share the dashboards with your users or embed them in your applications.

NEW QUESTION 39
Your company is planning on using bastion hosts for administering the servers in IAM. Which of the following is the best description of a bastion host from a security perspective?
Please select:

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

Answer: C

Explanation:
A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.
In IAM, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.
Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring For more information on bastion hosts, just browse to the below URL:
https://docsIAM.amazon.com/quickstart/latest/linux-bastion/architecture.htl
The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.
Submit your Feedback/Queries to our Experts

NEW QUESTION 40
A security team is working on a solution that will use Amazon EventBridge (Amazon CloudWatch Events) to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.
Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event. However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.
The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.
Which solution will meet these requirements?

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

Answer: D

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

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

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

› C. Enabling CloudTrail Insights to identify unusual API activity will not help the security team monitor new S3 objects or changes to any S3 bucket policy or setting that result in public access. CloudTrail Insights helps AWS users identify and respond to unusual activity associated with API calls and API error rates by continuously analyzing CloudTrail management events6. It does not analyze data events or generate EventBridge events.

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

NEW QUESTION 41
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 42
A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised. The instance was serving up malware. The analysis of the instance showed that the instance was compromised 35 days ago.
A security engineer must implement a continuous monitoring solution that automatically notifies the company's security team about compromised instances through an email distribution list for high severity findings. The security engineer must implement the solution as soon as possible.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

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

Answer: BCE

NEW QUESTION 44
Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets.
Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC. These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table.
The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.
How will the security engineer be able to comply with these requirements?

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

Answer: C

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

NEW QUESTION 48
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?

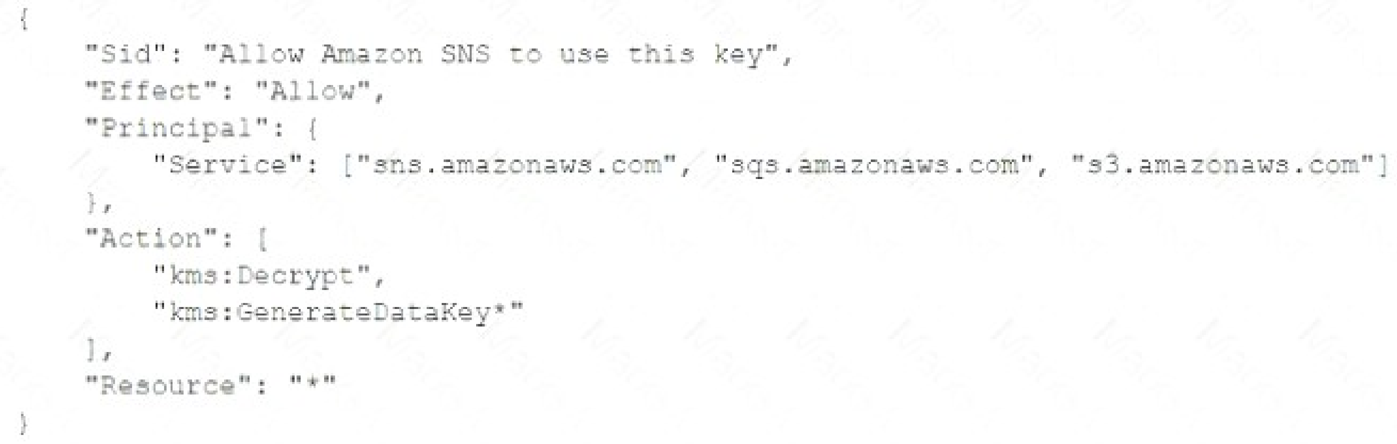
A. A customer managed CMK that uses customer provided key material
B. A customer managed CMK that uses AWS provided key material
C. An AWS managed CMK
D. Operation system-native encryption that uses GnuPG

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

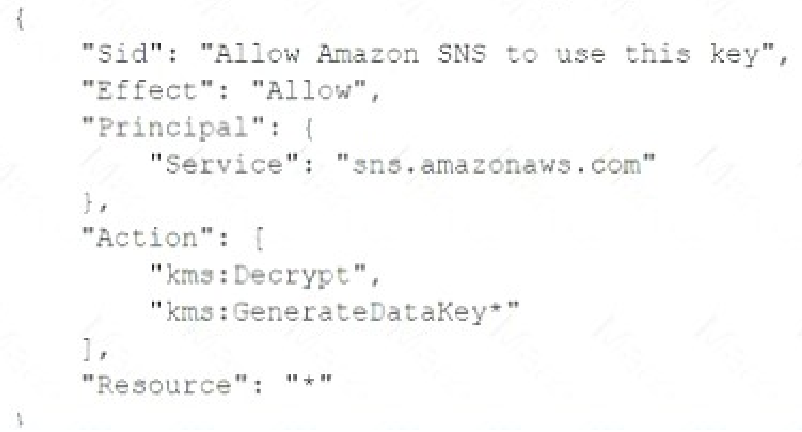
material to make the data inaccessible3.
* C. An AWS managed CMK is a KMS key that is created, owned, and managed by an AWS service on your behalf. You have limited control over the key configuration, permissions, rotation, and deletion. You cannot use an AWS managed CMK to encrypt data in other AWS 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 51
A Security Engineer is troubleshooting an issue with a company's custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events lo an Amazon SNS topic. All logs are encrypted at rest using an IAM KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.
The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No togs are being received.
What should the Security Engineer do to troubleshoot this issue?
A) Add the following statement to the IAM managed CMKs:



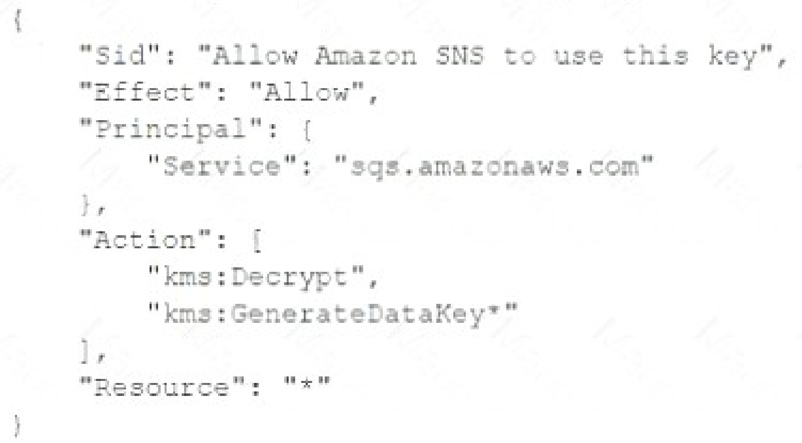
```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": ["sns.amazonaws.com", "sqs.amazonaws.com", "s3.amazonaws.com"]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

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



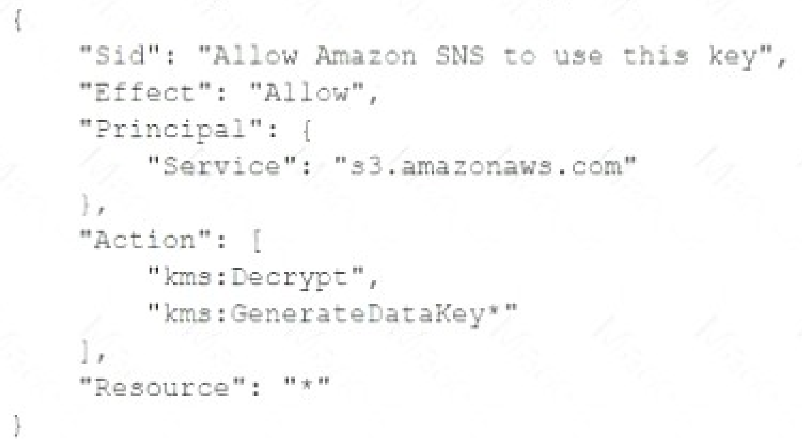
```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "sns.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

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



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

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



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

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

Answer: D

NEW QUESTION 52
A company is running an application in The eu-west-1 Region. The application uses an IAM Key Management Service (IAM KMS) CMK to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region.
A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code.
Which change should the security engineer make to the IAM KMS configuration to meet these requirements?

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

Answer: B

NEW QUESTION 53
A company needs a security engineer to implement a scalable solution for multi-account authentication and authorization. The solution should not introduce additional user-managed architectural components. Native IAM features should be used as much as possible The security engineer has set up IAM Organizations w1th all features activated and IAM SSO enabled.
Which additional steps should the security engineer take to complete the task?

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

Answer: B

NEW QUESTION 56
A company's security engineer is developing an incident response plan to detect suspicious activity in an AWS account for VPC hosted resources. The security engineer needs to provide visibility for as many AWS Regions as possible.
Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)

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

Answer: BD

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

NEW QUESTION 61
A company is building an application on IAM that will store sensitive Information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.
What should the security engineer recommend?

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

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

Answer: C

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

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

NEW QUESTION 63
A company's public Application Load Balancer (ALB) recently experienced a DDoS attack. To mitigate this issue. the company deployed Amazon CloudFront in front of the ALB so that users would not directly access the Amazon EC2 instances behind the ALB.
The company discovers that some traffic is still coming directly into the ALB and is still being handled by the EC2 instances.
Which combination of steps should the company take to ensure that the EC2 instances will receive traffic only from CloudFront? (Choose two.)

A. Configure CloudFront to add a cache key policy to allow a custom HTTP header that CloudFront sends to the ALB.
B. Configure CloudFront to add a custom: HTTP header to requests that CloudFront sends to the ALB.
C. Configure the ALB to forward only requests that contain the custom HTTP header.
D. Configure the ALB and CloudFront to use the X-Forwarded-For header to check client IP addresses.
E. Configure the ALB and CloudFront to use the same X.509 certificate that is generated by AWS Certificate Manager (ACM).

Answer: BC

Explanation:
To prevent users from directly accessing an Application Load Balancer and allow access only through CloudFront, complete these high-level steps: Configure CloudFront to add a custom HTTP header to requests that it sends to the Application Load Balancer. Configure the Application Load Balancer to only forward requests that contain the custom HTTP header. (Optional) Require HTTPS to improve the security of this solution.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html

NEW QUESTION 67
A company accidentally deleted the private key for an Amazon Elastic Block Store (Amazon EBS)-backed Amazon EC2 instance. A security engineer needs to regain access to the instance.
Which combination of steps will meet this requirement? (Choose two.)

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

Answer: AC

Explanation:
If you lose the private key for an EBS-backed instance, you can regain access to your instance. You must stop the instance, detach its root volume and attach it to another instance as a data volume, modify the authorized_keys file with a new public key, move the volume back to the original instance, and restart the instance.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#replacing

NEW QUESTION 72
A security engineer needs to see up an Amazon CloudFront distribution for an Amazon S3 bucket that hosts a static website. The security engineer must allow

only specified IP addresses to access the website. The security engineer also must prevent users from accessing the website directly by using S3 URLs.
Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 73
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 75
A company is running an Amazon RDS for MySQL DB instance in a VPC. The VPC must not send or receive network traffic through the internet.
A security engineer wants to use AWS Secrets Manager to rotate the DB instance credentials automatically. Because of a security policy, the security engineer cannot use the standard AWS Lambda function that Secrets Manager provides to rotate the credentials.
The security engineer deploys a custom Lambda function in the VPC. The custom Lambda function will be responsible for rotating the secret in Secrets Manager. The security engineer edits the DB instance's security group to allow connections from this function. When the function is invoked, the function cannot communicate with Secrets Manager to rotate the secret properly.
What should the security engineer do so that the function can rotate the secret?

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

Answer: D

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

- A. An egress-only internet gateway is a VPC component that allows outbound communication over IPv6 from instances in the VPC to the internet, and prevents the internet from initiating an IPv6 connection with the instances3. However, this option does not meet the requirement that the VPC must not send or receive network traffic through the internet. Moreover, an egress-only internet gateway is for use with IPv6 traffic only, and Secrets Manager does not support IPv6 addresses2.
- B. A NAT gateway is a VPC component that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections with those instances4. However, this option does not meet the requirement that the VPC must not send or receive network traffic through the internet. Additionally, a NAT gateway requires an elastic IP address, which is a public IPv4 address4.
- C. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses5. However, this option does not work because Secrets Manager does not have a default VPC that can be peered with. Furthermore, a VPC peering connection does not provide a private connection to Secrets Manager APIs without an internet gateway or other devices2.

NEW QUESTION 79
A company uses AWS Organizations. The company wants to implement short-term cre-dentials for third-party AWS accounts to use to access accounts within the com-pany's organization. Access is for the AWS Management Console and third-party software-as-a-service (SaaS) applications. Trust must be enhanced to prevent two external accounts from using the same credentials. The solution must require the least possible operational effort.
Which solution will meet these requirements?

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

Answer: D

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

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

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

Answer: C

NEW QUESTION 87
A company needs to store multiple years of financial records. The company wants to use Amazon S3 to store copies of these documents. The company must implement a solution to prevent the documents from being edited, replaced, or deleted for 7 years after the documents are stored in Amazon S3. The solution must also encrypt the documents at rest.
A security engineer creates a new S3 bucket to store the documents. What should the security engineer do next to meet these requirements?

A. Configure S3 server-side encryptio
B. Create an S3 bucket policy that has an explicit deny rule for all users for s3:DeleteObject and s3:PutObject API call
C. Configure S3 Object Lock to use governance mode with a retention period of 7 years.
D. Configure S3 server-side encryptio
E. Configure S3 Versioning on the S3 bucke
F. Configure S3 ObjectLock to use compliance mode with a retention period of 7 years.
G. Configure S3 Versionin
H. Configure S3 Intelligent-Tiering on the S3 bucket to move the documents to S3 Glacier Deep Archive storag
I. Use S3 server-side encryption immediatel
J. Expire the objects after 7 years.
K. Set up S3 Event Notifications and use S3 server-side encryptio
L. Configure S3 Event Notifications to target an AWS Lambda function that will review any S3 API call to the S3 bucket and deny the s3:DeleteObject and s3:PutObject API call
M. Remove the S3 event notification after 7 years.

Answer: B

NEW QUESTION 88
A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket direct.
Which solution will meet these requirements?

A. Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.
B. Create an origin access identity (OAI). Associate the OAI with the CloudFront distributio
C. Configure the S3 bucket permissions so that only the OAI can access the files in the S3 bucket.
D. Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.
E. Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

Answer: B

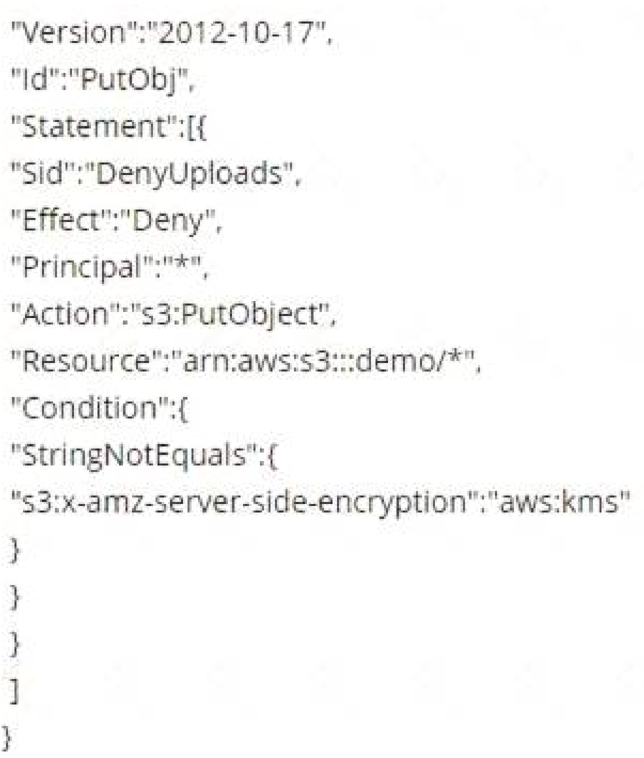
NEW QUESTION 92
A security engineer is working with a company to design an ecommerce application. The application will run on Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB). The application will use an Amazon RDS DB instance for its database.
The only required connectivity from the internet is for HTTP and HTTPS traffic to the application. The application must communicate with an external payment provider that allows traffic only from a preconfigured allow list of IP addresses. The company must ensure that communications with the external payment provider are not interrupted as the environment scales.
Which combination of actions should the security engineer recommend to meet these requirements? (Select THREE.)

A. Deploy a NAT gateway in each private subnet for every Availability Zone that is in use.
B. Place the DB instance in a public subnet.
C. Place the DB instance in a private subnet.
D. Configure the Auto Scaling group to place the EC2 instances in a public subnet.
E. Configure the Auto Scaling group to place the EC2 instances in a private subnet.
F. Deploy the ALB in a private subnet.

Answer: ACE

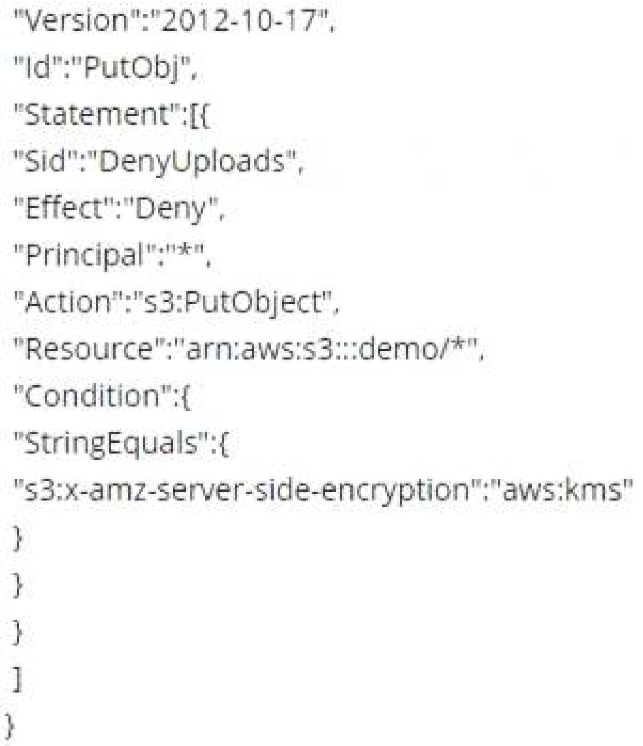
NEW QUESTION 95
Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.
Please select:

A. C:\Users\wk\Desktop\mudassar\Untitled.jpg



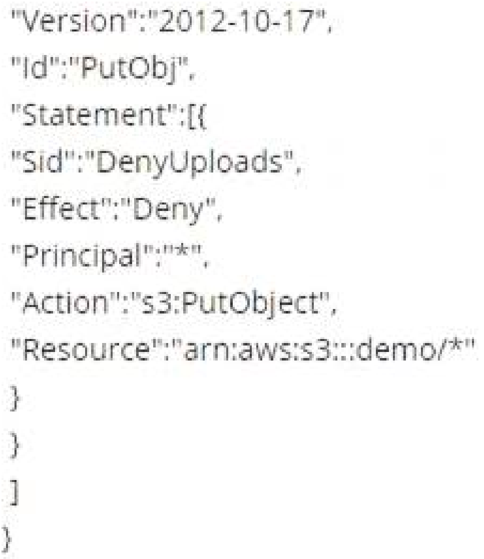
```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringNotEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}
```

B. C:\Users\wk\Desktop\mudassar\Untitled.jpg



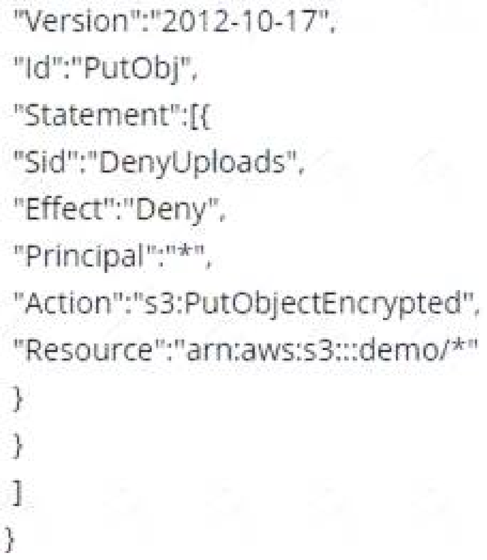
```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}
```

C. C:\Users\wk\Desktop\mudassar\Untitled.jpg



```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*"
}
}
]
}
```

D. C:\Users\wk\Desktop\mudassar\Untitled.jpg



```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObjectEncrypted",
"Resource":"arn:aws:s3:::demo/*"
}
}
]
}
```

Answer: A

Explanation:
The condition of "s3:x-amz-server-side-encryption":"IAM:kms" ensures that objects uploaded need to be encrypted.
Options B,C and D are invalid because you have to ensure the condition of ns3:x-amz-server-side-encryption":"IAM:kms" is present
For more information on IAM KMS best practices, just browse to the below URL: https://dl.IAMstatic.com/whitepapers/IAM-kms-best-praaices.pdf
Submit your Feedback/Queries to our Expert

NEW QUESTION 97
A company's security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.
Which solution will meet these requirements with the LEAST amount of effort?

A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hour
B. Select theaccess-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 day
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with an event pattern that matches the compliance type of NON_COMPLIANT from AWS Config for the managed rul
D. Configure EventBridge (CloudWatch Events) to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
E. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation.Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucke
F. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucke
G. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
H. Create a script to download the IAM credentials report on a periodic basi
I. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge (Amazon CloudWatch Events). Configure the Lambda script to load the report into memory and to filter the report for recordsin which the key was last rotated at least 90 days ag
J. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
K. Create an AWS Lambda function that queries the IAM API to list all the user
L. Iterate through the users by using the ListAccessKeys operatio
M. Verify that the value in the CreateDate field is not at least 90 days ol
N. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days ol
O. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule the Lambda function to run each day.

Answer: A

NEW QUESTION 99
A security engineer needs to run an AWS CloudFormation script. The CloudFormation script builds AWS infrastructure to support a stack that includes web servers and a MySQL database. The stack has been deployed in pre-production environments and is ready for production.
The production script must comply with the principle of least privilege. Additionally, separation of duties must exist between the security engineer's IAM account and CloudFormation.
Which solution will meet these requirements?

A. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stac
B. Attach the policy to a new IAM rol
C. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.
D. Create an IAM policy that allows ec2:* and rds:* permission

E. Attach the policy to a new IAM role.Modify the security engineer's IAM permissions to be able to assume the new role.
F. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stac
G. Modify the security engineer's IAM permissions to be able to run the CloudFormation script.
H. Create an IAM policy that allows ec2:* and rds:* permission
I. Attach the policy to a new IAM rol
J. Use the IAM policy simulator to confirm that the policy allows the AWS API calls that are necessary to build the stac
K. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.

Answer: A

Explanation:
The correct answer is A. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. Attach the policy to a new IAM role. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.
According to the AWS documentation, IAM Access Analyzer is a service that helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. You can also use IAM Access Analyzer to generate fine-grained policies that grant least privilege access based on access activity and access attempts.
To use IAM Access Analyzer policy generation, you need to enable IAM Access Analyzer in your account or organization. You can then use the IAM console or the AWS CLI to generate a policy for a resource based on its access activity or access attempts. You can review and edit the generated policy before applying it to the resource.
To use IAM Access Analyzer policy generation with CloudFormation, you can follow these steps:

- Run the CloudFormation script in a pre-production environment and monitor its access activity or access attempts using IAM Access Analyzer.
- Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. The policy will include only the permissions that are necessary for the script to function.
- Attach the policy to a new IAM role that has a trust relationship with CloudFormation. This will allow CloudFormation to assume the role and execute the script.
- Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.

This will allow the security engineer to launch the stack using the role.

- Run the CloudFormation script in the production environment using the new role.

This solution will meet the requirements of least privilege and separation of duties, as it will limit the permissions of both CloudFormation and the security engineer to only what is needed for running and managing the stack.
Option B is incorrect because creating an IAM policy that allows ec2:* and rds:* permissions is not following the principle of least privilege, as it will grant more permissions than necessary for running and managing the stack. Moreover, modifying the security engineer's IAM permissions to be able to assume the new role is not ensuring separation of duties, as it will allow the security engineer to bypass CloudFormation and directly access the resources.
Option C is incorrect because modifying the security engineer's IAM permissions to be able to run the CloudFormation script is not ensuring separation of duties, as it will allow the security engineer to execute the script without using CloudFormation.
Option D is incorrect because creating an IAM policy that allows ec2:* and rds:* permissions is not following the principle of least privilege, as it will grant more permissions than necessary for running and managing the stack. Using the IAM policy simulator to confirm that the policy allows the AWS API calls that are necessary to build the stack is not sufficient, as it will not generate a fine-grained policy based on access activity or access attempts.

NEW QUESTION 104
A company uses AWS Organizations. The company has teams that use an AWS CloudHSM hardware security module (HSM) that is hosted in a central AWS account. One of the teams creates its own new dedicated AWS account and wants to use the HSM that is hosted in the central account.
How should a security engineer share the HSM that is hosted in the central account with the new dedicated account?

A. Use AWS Resource Access Manager (AWS RAM) to share the VPC subnet ID of the HSM that is hosted in the central account with the new dedicated accoun
B. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.
C. Use AWS Identity and Access Management (IAM) to create a cross-account rote to access the CloudHSM cluster that is in the central account Create a new IAM user in the new dedicated account Assign the cross-account rote to the new IAM user.
D. Use AWS 1AM Identity Center (AWS Single Sign-On) to create an AWS Security Token Service (AWS STS) token to authenticate from the new dedicated account to the central accoun
E. Use thecross-account permissions that are assigned to the STS token to invoke an operation on the HSM in thecentral account.
F. Use AWS Resource Access Manager (AWS RAM) to share the ID of the HSM that is hosted in the central account with the new dedicated accoun
G. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.

Answer: A

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/cloudhsm-share-clusters/#:~:text=In%20the%20nav

NEW QUESTION 108
A developer 15 building a serverless application hosted on IAM that uses Amazon Redshift in a data store. The application has separate modules for read/write and read-only functionality. The modules need their own database users tor compliance reasons.
Which combination of steps should a security engineer implement to grant appropriate access' (Select TWO)

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

Answer: CD

Explanation:
To grant appropriate access to the application modules, the security engineer should do the following:

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

NEW QUESTION 109
A company uses Amazon EC2 Linux instances in the AWS Cloud. A member of the company's security team recently received a report about common vulnerability identifiers on the instances.
A security engineer needs to verify patching and perform remediation if the instances do not have the correct patches installed. The security engineer must determine which EC2 instances are at risk and must implement a solution to automatically update those instances with the applicable patches.
What should the security engineer do to meet these requirements?

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

Answer: A

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

NEW QUESTION 112
An international company has established a new business entity in South Korea. The company also has established a new AWS account to contain the workload for the South Korean region. The company has set up the workload in the new account in the ap-northeast-2 Region. The workload consists of three Auto Scaling groups of Amazon EC2 instances. All workloads that operate in this Region must keep system logs and application logs for 7 years.
A security engineer must implement a solution to ensure that no logging data is lost for each instance during scaling activities. The solution also must keep the logs for only the required period of 7 years.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

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

Answer: ABC

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

NEW QUESTION 113
A company is deploying an Amazon EC2-based application. The application will include a custom health-checking component that produces health status data in JSON format. A Security Engineer must
implement a secure solution to monitor application availability in near-real time by analyzing the hearth status data.
Which approach should the Security Engineer use?

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

Answer: A

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

NEW QUESTION 118
A company uses several AWS CloudFormation stacks to handle the deployment of a suite of applications. The leader of the company's application development team notices that the stack deployments fail with permission errors when some team members try to deploy the stacks. However, other team members can deploy the stacks successfully.
The team members access the account by assuming a role that has a specific set of permissions that are necessary for the job responsibilities of the team members. All team members have permissions to perform operations on the stacks.
Which combination of steps will ensure consistent deployment of the stacks MOST securely? (Select THREE.)

A. Create a service role that has a composite principal that contains each service that needs the necessary permission
B. Configure the role to allow the sts:AssumeRole action.
C. Create a service role that has cloudformation.amazonaws.com as the service principa
D. Configure the role to allow the sts:AssumeRole action.
E. For each required set of permissions, add a separate policy to the role to allow those permission
F. Add the ARN of each CloudFormation stack in the resource field of each policy.
G. For each required set of permissions, add a separate policy to the role to allow those permission
H. Add the ARN of each service that needs the per-missions in the resource field of the corresponding policy.
I. Update each stack to use the service role.
J. Add a policy to each member role to allow the iam:PassRole actio
K. Set the policy's resource field to the ARN of the service role.

Answer: BDF

NEW QUESTION 123
A company needs to retain tog data archives for several years to be compliant with regulations. The tog data is no longer used but It must be retained
What Is the MOST secure and cost-effective solution to meet these requirements?

A. Archive the data to Amazon S3 and apply a restrictive bucket policy to deny the s3 DeleteOotect API
B. Archive the data to Amazon S3 Glacier and apply a Vault Lock policy
C. Archive the data to Amazon S3 and replicate it to a second bucket in a second IAM Region Choose the S3 Standard-Infrequent Access (S3 Standard-1A) storage class and apply a restrictive bucket policy to deny the s3 DeleteObject API
D. Migrate the log data to a 16 T8 Amazon Elastic Block Store (Amazon EBS) volume Create a snapshot of the EBS volume

Answer: B

Explanation:
To securely and cost-effectively retain log data archives for several years, the company should do the following:
- Archive the data to Amazon S3 Glacier and apply a Vault Lock policy. This allows the company to use a low-cost storage class that is designed for long-term archival of data that is rarely accessed. It also allows the company to enforce compliance controls on their S3 Glacier vault by locking a vault access policy that cannot be changed.

NEW QUESTION 125
A company has several petabytes of data. The company must preserve this data for 7 years to comply with regulatory requirements. The company's compliance team asks a security officer to develop a strategy that will prevent anyone from changing or deleting the data.
Which solution will meet this requirement MOST cost-effectively?

A. Create an Amazon S3 bucke
B. Configure the bucket to use S3 Object Lock in compliance mod
C. Upload the data to the bucke
D. Create a resource-based bucket policy that meets all the regulatory requirements.
E. Create an Amazon S3 bucke
F. Configure the bucket to use S3 Object Lock in governance mod
G. Upload the data to the bucke
H. Create a user-based IAM policy that meets all the regulatory requirements.
I. Create a vault in Amazon S3 Glacie
J. Create a Vault Lock policy in S3 Glacier that meets all the regulatory requirement
K. Upload the data to the vault.
L. Create an Amazon S3 bucke
M. Upload the data to the bucke
N. Use a lifecycle rule to transition the data to a vault in S3 Glacie
O. Create a Vault Lock policy that meets all the regulatory requirements.

Answer: C

Explanation:
To preserve the data for 7 years and prevent anyone from changing or deleting it, the security officer needs to use a service that can store the data securely and enforce compliance controls. The most cost-effective way to do this is to use Amazon S3 Glacier, which is a low-cost storage service for data archiving and long-term backup. S3 Glacier allows you to create a vault, which is a container for storing archives. Archives are any data such as photos, videos, or documents that you want to store durably and reliably.
S3 Glacier also offers a feature called Vault Lock, which helps you to easily deploy and enforce compliance controls for individual vaults with a Vault Lock policy. You can specify controls such as “write once read many” (WORM) in a Vault Lock policy and lock the policy from future edits. Once a Vault Lock policy is locked, the policy can no longer be changed or deleted. S3 Glacier enforces the controls set in the Vault Lock policy to help achieve your compliance objectives. For example, you can use Vault Lock policies to enforce data retention by denying deletes for a specified period of time.
To use S3 Glacier and Vault Lock, the security officer needs to follow these steps:
- Create a vault in S3 Glacier using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS SDKs.
- Create a Vault Lock policy in S3 Glacier that meets all the regulatory requirements using the IAM policy language. The policy can include conditions such as aws:CurrentTime or aws:SecureTransport to further restrict access to the vault.
- Initiate the lock by attaching the Vault Lock policy to the vault, which sets the lock to an in-progress state and returns a lock ID. While the policy is in the in-progress state, you have 24 hours to validate
your Vault Lock policy before the lock ID expires. To prevent your vault from exiting the in-progress state, you must complete the Vault Lock process within these

24 hours. Otherwise, your Vault Lock policy will be deleted.

- Use the lock ID to complete the lock process. If the Vault Lock policy doesn't work as expected, you can stop the Vault Lock process and restart from the beginning.
- Upload the data to the vault using either direct upload or multipart upload methods. For more information about S3 Glacier and Vault Lock, see S3 Glacier Vault Lock.

The other options are incorrect because:

- Option A is incorrect because creating an Amazon S3 bucket and configuring it to use S3 Object Lock in compliance mode will not prevent anyone from changing or deleting the data. S3 Object Lock is a feature that allows you to store objects using a WORM model in S3. You can apply two types of object locks: retention periods and legal holds. A retention period specifies a fixed period of time during which an object remains locked. A legal hold is an indefinite lock on an object until it is removed. However, S3 Object Lock only prevents objects from being overwritten or deleted by any user, including the root user in your AWS account. It does not prevent objects from being modified by other means, such as changing their metadata or encryption settings. Moreover, S3 Object Lock requires that you enable versioning on your bucket, which will incur additional storage costs for storing multiple versions of an object.
- Option B is incorrect because creating an Amazon S3 bucket and configuring it to use S3 Object Lock in governance mode will not prevent anyone from changing or deleting the data. S3 Object Lock in governance mode works similarly to compliance mode, except that users with specific IAM permissions can change or delete objects that are locked. This means that users who have s3:BypassGovernanceRetention permission can remove retention periods or legal holds from objects and overwrite or delete them before they expire. This option does not provide strong enforcement for compliance controls as required by the regulatory requirements.
- Option D is incorrect because creating an Amazon S3 bucket and using a lifecycle rule to transition the data to a vault in S3 Glacier will not prevent anyone from changing or deleting the data. Lifecycle rules are actions that Amazon S3 automatically performs on objects during their lifetime. You can use lifecycle rules to transition objects between storage classes or expire them after a certain period of time. However, lifecycle rules do not apply any compliance controls on objects or prevent them from being modified or deleted by users. Moreover, transitioning objects from S3 to S3 Glacier using lifecycle rules will incur additional charges for retrieval requests and data transfers.

NEW QUESTION 126

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

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

Answer: D

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

NEW QUESTION 130

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

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

Answer: A

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

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

NEW QUESTION 132

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

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

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

Answer: D

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

NEW QUESTION 136
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 137
A security engineer is designing a cloud architecture to support an application. The application runs on Amazon EC2 instances and processes sensitive information, including credit card numbers.
The application will send the credit card numbers to a component that is running in an isolated environment. The component will encrypt, store, and decrypt the numbers.
The component then will issue tokens to replace the numbers in other parts of the application.
The component of the application that manages the tokenization process will be deployed on a separate set of EC2 instances. Other components of the application must not be able to store or access the credit card numbers.
Which solution will meet these requirements?

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

Answer: D

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

NEW QUESTION 141
A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.
Which solution will meet these requirements with the LEAST operational overhead?

A. Configure the S3 Block Public Access feature for the AWS account.
B. Configure the S3 Block Public Access feature for all objects that are in the bucket.
C. Deactivate ACLs for objects that are in the bucket.
D. Use AWS PrivateLink for Amazon S3 to access the bucket.

Answer: D

NEW QUESTION 143
A company has deployed Amazon GuardDuty and now wants to implement automation for potential threats. The company has decided to start with RDP brute force attacks that come from Amazon EC2 instances in the company’s AWS environment. A security engineer needs to implement a solution that blocks the detected communication from a suspicious instance until investigation and potential remediation can occur.
Which solution will meet these requirements?

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

Answer: C

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

NEW QUESTION 147
A company wants to configure DNS Security Extensions (DNSSEC) for the company's primary domain. The company registers the domain with Amazon Route 53. The company hosts the domain on Amazon EC2 instances by using BIND.
What is the MOST operationally efficient solution that meets this requirement?

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

Answer: D

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

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

NEW QUESTION 148
A company is developing an ecommerce application. The application uses Amazon EC2 instances and an Amazon RDS MySQL database. For compliance reasons, data must be secured in transit and at rest. The company needs a solution that minimizes operational overhead and minimizes cost.
Which solution meets these requirements?

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

Answer: A

NEW QUESTION 150
......