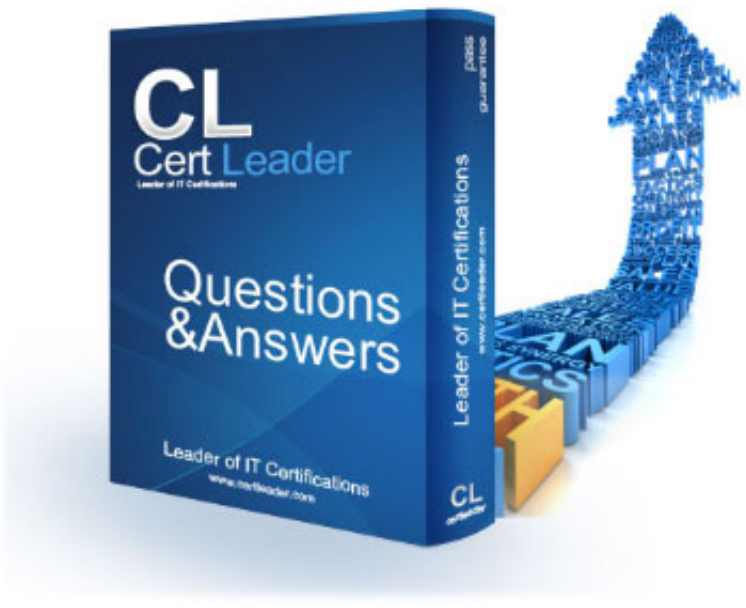
SCS-C02 Dumps

AWS Certified Security - Specialty

https://www.certleader.com/SCS-C02-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
A security engineer has created an Amazon Cognito user pool. The engineer needs to manually verify the ID and access token sent by the application for troubleshooting purposes
What is the MOST secure way to accomplish this?

A. Extract the subject (sub), audience (aud), and cognito:username from the ID token payload Manually check the subject and audience for the user name In the user pool
B. Search for the public key with a key ID that matches the key ID In the header of the toke
C. Then use a JSON Web Token (JWT) library to validate the signature of the token and extract values, such as the expiry date
D. Verify that the token is not expire
E. Then use the token_use claim function In Amazon Cognito to validate the key IDs
F. Copy the JSON Web Token (JWT) as a JSON document Obtain the public JSON Web Key (JWK) and convert It to a pem fil
G. Then use the file to validate the original JWT.

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
A Developer reported that IAM CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.
What should the Security Engineer do to meet these requirements?

A. Use IAM Resource Access Manager (IAM RAM) to monitor the IAM CloudTrail configuratio
B. Send notifications using Amazon SNS.
C. Create an Amazon CloudWatch Events rule to monitor Amazon GuardDuty finding
D. Send email notifications using Amazon SNS.
E. Update security contact details in IAM account settings for IAM Support to send alerts when suspicious activity is detected.
F. Use Amazon Inspector to automatically detect security issue
G. Send alerts using Amazon SNS.

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
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 IAM 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 IAM Key Management Services to encrypt all the traffic between the client and application servers.

Answer: BD

NEW QUESTION 4
- (Exam Topic 1)
A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.
After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the IAM account was compromised and Amazon EBS snapshots were deleted.
All EBS snapshots are encrypted using an IAM KMS CMK. Which solution would solve this problem?

A. Create a new Amazon S3 bucket Use EBS lifecycle policies to move EBS snapshots to the new S3 bucke
B. Move snapshots to Amazon S3 Glacier using lifecycle policies, and apply Glacier Vault Lock policies to prevent deletion
C. Use IAM Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.
D. Create a new IAM account with limited privilege
E. Allow the new account to access the IAM KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recuning basis
F. Use IAM Backup to copy EBS snapshots to Amazon S3.

Answer: A

NEW QUESTION 5
- (Exam Topic 1)
A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running In Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns
Which solution would have the MOST scalability and LOWEST latency?

A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers
D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
A company has a VPC with several Amazon EC2 instances behind a NAT gateway. The company's security policy states that all network traffic must be logged and must include the original source and destination IP addresses. The existing VPC Flow Logs do not include this information. A security engineer needs to recommend a solution.
Which combination of steps should the security engineer recommend? (Select TWO)

A. Edit the existing VPC Flow Log
B. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
C. Delete and recreate the existing VPC Flow Log
D. Change the log format of the VPC Flow Logs from the Amazon default format to a custom format.
E. Change the destination to Amazon CloudWatch Logs.
F. Include the pkt-srcaddr and pkt-dstaddr fields in the log format.
G. Include the subnet-id and instance-id fields in the log format.

Answer: AE

NEW QUESTION 7
- (Exam Topic 1)
A company recently performed an annual security assessment of its IAM environment. The assessment showed that audit logs are not available beyond 90 days and that unauthorized changes to IAM policies are made without detection.
How should a security engineer resolve these issues?

A. Create an Amazon S3 lifecycle policy that archives IAM CloudTrail trail logs to Amazon S3 Glacier after 90 day
B. Configure Amazon Inspector to provide a notification when a policy change is made to resources.
C. Configure IAM Artifact to archive IAM CloudTrail logs Configure IAM Trusted Advisor to provide a notification when a policy change is made to resources.
D. Configure Amazon CloudWatch to export log groups to Amazon S3. Configure IAM CloudTrail to provide a notification when a policy change is made to resources.
E. Create an IAM CloudTrail trail that stores audit logs in Amazon S3. Configure an IAM Config rule to provide a notification when a policy change is made to resources.

Answer: D

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/best-practices-security.html
"For an ongoing record of events in your IAM account, you must create a trail. Although CloudTrail provides 90 days of event history information for management events in the CloudTrail console without creating a trail, it is not a permanent record, and it does not provide information about all possible types of events. For an ongoing record, and for a record that contains all the event types you specify, you must create a trail, which delivers log files to an Amazon S3 bucket that you specify."
https://IAM.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-IAM

NEW QUESTION 8
- (Exam Topic 1)
A company's security engineer is configuring Amazon S3 permissions to ban all current and future public buckets However, the company hosts several websites directly off S3 buckets with public access enabled
The engineer needs to bock me pubic S3 buckets without causing any outages on me easting websites The engineer has set up an Amazon CloudFrom distribution (or each website
Which set or steps should the security engineer implement next?

A. Configure an S3 bucket as the origin an origin access identity (OAI) for the CloudFront distribution Switch the DNS records from websites to point to the CloudFront distribution Enable Nock public access settings at the account level
B. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Switch the ONS records tor the websites to point to the CloudFront disinfection Then, tor each S3 bucket enable block public access settings
C. Configure an S3 bucket as the origin with an origin access identity (OAI) for the CloudFront distribution Enable block public access settings at the account level
D. Configure an S3 bucket as the origin for me CloudFront distribution Configure the S3 bucket policy to accept connections from the CloudFront points of presence only Switch the DNS records for the websites to point to the CloudFront distribution Enable block public access settings at me account level

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from IAM stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.
How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

A. Give consent to the IAM Security team to dump the memory core on the compromised instance and provide it to IAM Support for analysis.
B. Review memory dump data that the IAM Systems Manager Agent sent to Amazon CloudWatch Logs.
C. Download and run the EC2Rescue for Windows Server utility from IAM.
D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

Answer: C

Explanation:
https://docs.IAM.amazon.com/IAMEC2/latest/WindowsGuide/ec2rw-cli.html

NEW QUESTION 10
- (Exam Topic 1)

A company wants to encrypt the private network between its orvpremises environment and IAM. The company also wants a consistent network experience for its employees.
What should the company do to meet these requirements?

A. Establish an IAM Direct Connect connection with IAM and set up a Direct Connect gatewa
B. In the Direct Connect gateway configuration, enable IPsec and BGP, and then leverage native IAM network encryption between Availability Zones and Regions,
C. Establish an IAM Direct Connect connection with IAM and set up a Direct Connect gatewa
D. Using the Direct Connect gateway, create a private virtual interface and advertise the customer gateway private IP addresse
E. Create a VPN connection using the customer gateway and the virtual private gateway
F. Establish a VPN connection with the IAM virtual private cloud over the internet
G. Establish an IAM Direct Connect connection with IAM and establish a public virtual interfac
H. For prefixes that need to be advertised, enter the customer gateway public IP addresse
I. Create a VPN connection over Direct Connect using the customer gateway and the virtual private gateway.

Answer: D

NEW QUESTION 10
- (Exam Topic 1)
After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Principal":"*",
            "Action":"s3:*",
            "Resource":"arn:aws:s3:::examplebucket/*",
            "Condition":{
                "IpAddress":{
                    "aws:SourceIp":[
                        "10.10.10.0/24"
                    ]
                }
            }
        }
    ]
}
```

Is this bucket policy sufficient to ensure that the data is not publicity accessible?

A. Yes, the bucket policy makes the whole bucket publicly accessible despite now the S3 bucket ACL or object ACLs are configured.
B. Yes, none of the data in the bucket is publicity accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.
D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

Answer: A

NEW QUESTION 15
- (Exam Topic 1)
A company uses Microsoft Active Directory for access management for on-premises resources and wants to use the same mechanism for accessing its IAM accounts. Additionally, the development team plans to launch a public-facing application for which they need a separate authentication solution.
When coma nation of the following would satisfy these requirements? (Select TWO)

A. Set up domain controllers on Amazon EC2 to extend the on-premises directory to IAM
B. Establish network connectivity between on-premises and the user's VPC
C. Use Amazon Cognito user pools for application authentication
D. Use AD Connector tor application authentication.
E. Set up federated sign-in to IAM through ADFS and SAML.

Answer: CD

NEW QUESTION 20
- (Exam Topic 1)
A company uses multiple IAM accounts managed with IAM Organizations Security engineers have created a standard set of security groups for all these accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only.
A recent security audit found that the security groups are inconsistency implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.
Which solution should the security engineer recommend?

A. Use IAM Resource Access Manager to create shared resources for each requited security group and apply an IAM policy that permits read-only access to the security groups only.
B. Create an IAM CloudFormation template that creates the required security groups Execute the template as part of configuring new accounts Enable Amazon Simple Notification Service (Amazon SNS) notifications when changes occur
C. Use IAM Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation
D. Use IAM Control Tower to edit the account factory template to enable the snare security groups option Apply an SCP to the OU or individual accounts that prohibits security group modifications from local account users

Answer: B

NEW QUESTION 24

- (Exam Topic 1)
A company is designing the securely architecture (or a global latency-sensitive web application it plans to deploy to IAM. A Security Engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.
Which solution meets these requirements?

A. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Regio
B. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
C. Create an AmazonCloudFront distribution that uses the ALB as its origi
D. Create appropriate IAM WAF ACLs and enable them on the CloudFront distribution.
E. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Regio
F. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
G. Create an Amazon CloudFront distribution that uses the ALB as its origi
H. Create appropriate IAM WAF ACLs and enable them on the CloudFront distribution.
I. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Regio
J. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
K. Create appropriate IAM WAF ACLs and enable them on the ALB.
L. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Regio
M. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Regio
N. Create appropriate IAM WAF ACLs and enable them on the ALB.

Answer: A

NEW QUESTION 25
- (Exam Topic 1)
Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the internet. The connection either fails to respond or generates the following error message:
Network error: Connection timed out.
What could be responsible for the connection failure? (Select THREE)

A. The NAT gateway in the subnet where the EC2 instance is deployed has been misconfigured
B. The internet gateway of the VPC has been reconfigured
C. The security group denies outbound traffic on ephemeral ports
D. The route table is missing a route to the internet gateway
E. The NACL denies outbound traffic on ephemeral ports
F. The host-based firewall is denying SSH traffic

Answer: BDF

NEW QUESTION 29
- (Exam Topic 1)
A Security Engineer is troubleshooting a connectivity issue between a web server that is writing log files to the logging server in another VPC. The Engineer has confirmed that a peering relationship exists between the two VPCs. VPC flow logs show that requests sent from the web server are accepted by the togging server but the web server never receives a reply
Which of the following actions could fix this issue1?

A. Add an inbound rule to the security group associated with the logging server that allows requests from the web server
B. Add an outbound rule to the security group associated with the web server that allows requests to the logging server.
C. Add a route to the route table associated with the subnet that hosts the logging server that targets the peering connection
D. Add a route to the route table associated with the subnet that hosts the web server that targets the peering connection

Answer: C

NEW QUESTION 33
- (Exam Topic 1)
A company's Director of information Security wants a daily email report from IAM that contains recommendations for each company account to meet IAM Security best practices.
Which solution would meet these requirements?

A. in every IAM account, configure IAM Lambda to query me IAM Support API tor IAM Trusted Advisor security checks Send the results from Lambda to an Amazon SNS topic to send reports.
B. Configure Amazon GuardDuty in a master account and invite all other accounts to be managed by the master account Use GuardDuty's integration with Amazon SNS to report on findings
C. Use Amazon Athena and Amazon QuickSight to build reports off of IAM CloudTrail Create a daily Amazon CloudWatch trigger to run the report dally and email It using Amazon SNS
D. Use IAM Artifact's prebuilt reports and subscriptions Subscribe the Director of Information Security to the reports by adding the Director as the security alternate contact tor each account

Answer: A

NEW QUESTION 38
- (Exam Topic 1)
A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other IAM account resources by using the EC2 instance metadata service.
What can the Administrator do to protect against this potential attack?

A. Disable the EC2 instance metadata service.
B. Log all student SSH interactive session activity.
C. Implement ip tables-based restrictions on the instances.

D. Install the Amazon Inspector agent on the instances.

Answer: A

Explanation:
"To turn off access to instance metadata on an existing instance....." https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/configuring-instance-metadata-service.html You can disable the service for existing (running or stopped) ec2 instances. https://docs.IAM.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html

NEW QUESTION 42
- (Exam Topic 1)
A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An IAM WAF web ACL is associated with the ALB. IAM CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.
The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.
Which set of actions will identify the suspect attacker's IP address for future occurrences?

A. Configure VPC Flow Logs on the subnet where the ALB is located, and stream the data CloudWatch.Search for the new-user-creation.php occurrences in CloudWatch.
B. Configure the CloudWatch agent on the ALB Configure the agent to send application logs to CloudWatch Update the instance role to allow CloudWatch Logs acces
C. Export the logs to CloudWatch Search for the new-user-creation.php occurrences in CloudWatch.
D. Configure the ALB to export access logs to an Amazon Elasticsearch Service cluster, and use the service to search for the new-user-creation.php occurrences.
E. Configure the web ACL to send logs to Amazon Kinesis Data Firehose, which delivers the logs to an S3 bucket Use Amazon Athena to query the logs and find the new-user-creation php occurrences.

Answer: D

Explanation:
You send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, IAM WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose. https://docs.IAM.amazon.com/waf/latest/developerguide/logging.html

NEW QUESTION 45
- (Exam Topic 1)
A company has the software development teams that are creating applications that store sensitive data in Amazon S3 Each team's data must always be separate. The company's security team must design a data encryption strategy for both teams that provides the ability to audit key usage. The solution must also minimize operational overhead
what should me security team recommend?

A. Tell the application teams to use two different S3 buckets with separate IAM Key Management Service (IAM KMS) IAM managed CMKs Limit the key process to allow encryption and decryption of the CMKs to their respective teams onl
B. Force the teams to use encryption context to encrypt and decrypt
C. Tell the application teams to use two different S3 buckets with a single IAM Key Management Service (IAM KMS) IAM managed CMK Limit the key policy to allow encryption and decryption of the CMK onl
D. Do not allow the teams to use encryption context to encrypt and decrypt
E. Tell the application teams to use two different S3 buckets with separate IAM Key Management Service (IAM KMS) customer managed CMKs Limit the key policies to allow encryption and decryption of the CMKs to their respective teams only Force the teams to use encryption context to encrypt and decrypt
F. Tell the application teams to use two different S3 buckets with a single IAM Key Management Service (IAM KMS) customer managed CMK Limit the key policy to allow encryption and decryption of the CMK only Do not allow the teams to use encryption context to encrypt and decrypt

Answer: A

NEW QUESTION 50
- (Exam Topic 1)
A recent security audit identified that a company's application team injects database credentials into the environment variables of an IAM Fargate task. The company's security policy mandates that all sensitive data be encrypted at rest and in transit.
When combination of actions should the security team take to make the application compliant within the security policy? (Select THREE)

A. Store the credentials securely in a file in an Amazon S3 bucket with restricted access to the application team IAM role Ask the application team to read the credentials from the S3 object instead
B. Create an IAM Secrets Manager secret and specify the key/value pairs to be stored in this secret
C. Modify the application to pull credentials from the IAM Secrets Manager secret instead of the environment variables.
D. Add the following statement to the container instance IAM role policy

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

E. Add the following statement to the execution role policy.

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

F. Log in to the IAM Fargate instance, create a script to read the secret value from IAM Secret Manager, and inject the environment variable
G. Ask the application team to redeploy the application.

Answer: BEF

NEW QUESTION 53
- (Exam Topic 1)
A security engineer must use IAM Key Management Service (IAM 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 IAM provided key material
C. An IAM managed CMK
D. Operating system-native encryption that uses GnuPG

Answer: B

NEW QUESTION 54
- (Exam Topic 1)
A Developer signed in to a new account within an IAM Organizations organizations unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

How can the Security Engineer provide the Developer with Amazon S3 access without affecting other accounts?

A. Move the SCP to the root OU of Organizations to remove the restriction to access Amazon S3.
B. Add an IAM policy for the Developer, which grants S3 access.
C. Create a new OU without applying the SCP restricting S3 acces
D. Move the Developer account to this new OU.
E. Add an allow list for the Developer account for the S3 service.

Answer: C

NEW QUESTION 56
- (Exam Topic 1)
A company has a VPC with an IPv6 address range and a public subnet with an IPv6 address block. The VPC currently hosts some public Amazon EC2 instances but a Security Engineer needs to migrate a second application into the VPC that also requires IPv6 connectivity.
This new application will occasionally make API requests to an external, internet-accessible endpoint to receive updates However, the Security team does not want the application's EC2 instance exposed directly to the internet The Security Engineer intends to create a private subnet with a custom route table and to associate the route table with the private subnet
What else does the Security Engineer need to do to ensure the application will not be exposed directly to the internet, but can still communicate as required"

A. Launch a NAT instance in the public subnet Update the custom route table with a new route to the NAT instance
B. Remove the internet gateway, and add IAM PrivateLink to the VPC Then update the custom route table with a new route to IAM PrivateLink
C. Add a managed NAT gateway to the VPC Update the custom route table with a new route to the gateway
D. Add an egress-only internet gateway to the VP
E. Update the custom route table with a new route to thegateway

Answer: D

NEW QUESTION 61
- (Exam Topic 1)
A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data All logs must be kept for a minimum of 1 year for auditing purposes
What should the security engineer recommend?

A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is

create
B. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
C. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
D. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling grou
E. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.
F. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer: B

NEW QUESTION 64
- (Exam Topic 1)
A developer is creating an IAM Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an IAM KMS Customer Master Key (CMK> supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.
Which of the following are required for this configuration to work? (Select TWO.)

A. The developer must configure Lambda access to the VPC using the --vpc-config parameter.
B. The Lambda function execution role must have the kms:Decrypt- permission added in the IAM IAM policy.
C. The KMS key policy must allow permissions for the developer to use the KMS key.
D. The IAM IAM policy assigned to the developer must have the kmseGcnerate-DataKcy permission added.
E. The Lambda execution role must have the kms:Encrypt permission added in the IAM IAM policy.

Answer: BC

NEW QUESTION 66
- (Exam Topic 1)
A security engineer has noticed that VPC Flow Logs are getting a lot REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.
What immediate action should the security engineer take? What immediate action should the security engineer take?

A. Remove me instance from the Auto Seating group Close me security group mm ingress only from a single forensic P address to perform an analysis.
B. Remove me instance from the Auto Seating group Change me network ACL rules to allow traffic only from a single forensic IP address to perform en analysis Add a rule to deny all other traffic.
C. Remove the instance from the Auto Scaling group Enable Amazon GuardDuty in that IAM account Install the Amazon Inspector agent cm the suspicious EC 2 instance to perform a scan.
D. Take a snapshot of the suspicious EC2 instanc
E. Create a new EC2 instance from me snapshot in a closed security group with ingress only from a single forensic IP address to perform an analysis

Answer: B

NEW QUESTION 69
- (Exam Topic 1)
Two Amazon EC2 instances in different subnets should be able to connect to each other but cannot. It has been confirmed that other hosts in the same subnets are able to communicate successfully, and that security groups have valid ALLOW rules in place to permit this traffic.
Which of the following troubleshooting steps should be performed?

A. Check inbound and outbound security groups, looking for DENY rules.
B. Check inbound and outbound Network ACL rules, looking for DENY rules.
C. Review the rejected packet reason codes in the VPC Flow Logs.
D. Use IAM X-Ray to trace the end-to-end application flow

Answer: C

NEW QUESTION 71
- (Exam Topic 1)
An application developer is using an IAM Lambda function that must use IAM KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB
Which key policy would allow the application to do this while granting least privilege?

A.
```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:*"
 ],
 "Resource": "*"
}
```

B.
```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:Encrypt",
  "kms:Decrypt"
 ],
 "Resource": "*"
}
```

C.
```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:DescribeKey",
  "kms:GenerateDataKey*",
  "kms:Encrypt",
  "kms:ReEncrypt*",
  "kms:Decrypt"
```

D.
```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:DescribeKey",
  "kms:GenerateDataKey*",
  "kms:Encrypt",
  "kms:ReEncrypt*",
  "kms:Disable*",
  "kms:Decrypt"
 ],
```

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

Answer: C

NEW QUESTION 73
- (Exam Topic 1)
A company plans to use custom AMIs to launch Amazon EC2 instances across multiple IAM accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed IAM KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups.
Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute tasks?

A. Create a customer-managed CMK in the centralized accoun
B. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
C. Create an IAM role in all applicable accounts and configure its access policy to allow the use of the centrally managed CMK for cryptographical operation
D. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.
E. Create a customer-managed CMK in the centralized accoun
F. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
G. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CM
H. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographical operations and with the EC2 Auto Scalingservice-linked role defined as the grantee principal.
I. Create a customer-managed CMK or an IAM managed CMK in the centralized accoun
J. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
K. Use the CMK administrator to create a CMK grant that includes permissions to perform cryptographical operations that define EC2 Auto Scaling service-linked roles from all other accounts as the grantee principal.
L. Create a customer-managed CMK or an IAM managed CMK in the centralized accoun
M. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key polic
N. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographical operations against the centrally managed CMK.

Answer: B

NEW QUESTION 76
- (Exam Topic 1)
A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

A. Associate the instances to the same security groups.
B. Add 0.0.0.0/0 to the egress rules of the instance security groups.
C. Add the instance IDs to the ingress rules of the instance security groups.
D. Add the public IP addresses to the ingress rules of the instance security groups.

Answer: D

Explanation:
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-in

NEW QUESTION 79
- (Exam Topic 2)
During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.
What could have been done to detect and automatically remediate the incident?

A. Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to IAM CloudTrail, and revoke the new API keys for the root user.
B. Using IAM Config, create a config rule that detects when IAM CloudTrail is disabled, as well as any calls to the root user create-api-ke
C. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.
D. Using Amazon CloudWatch, create a CloudWatch event that detects IAM CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API key
E. Then use a Lambda function to enable IAM CloudTrail and deactivate the root API keys.
F. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API key
G. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

Answer: B

Explanation:
https://docs.IAM.amazon.com/config/latest/developerguide/cloudtrail-enabled.html https://docs.IAM.amazon.com/config/latest/developerguide/iam-root-access-key-check.html

NEW QUESTION 80
- (Exam Topic 2)
During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.
What solution will allow the Security team to complete this request?

A. Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier functio
B. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.
C. Enable Amazon Macie on the S3 buckets that were impacted, then perform data classificatio
D. For identified objects that contain PII, use the research function for auditing IAM CloudTrail logs and S3 bucket logs for GET operations.
E. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classificatio
F. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
G. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classificatio
H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer: B

NEW QUESTION 83
- (Exam Topic 2)
You have an S3 bucket hosted in IAM. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?
Please select:

A. Use versioning and enable a timestamp for each version
B. Use Pre-signed URL's
C. Use IAM Roles with a timestamp to limit the access
D. Use IAM policies with a timestamp to limit the access

Answer: B

Explanation:
The IAM Documentation mentions the following
All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.
Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles
Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:
https://docs.IAM.ama2on.com/AmazonS3/latest/dev/ShareObiectPreSisnedURL.html
The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 88
- (Exam Topic 2)
You have an instance setup in a test environment in IAM. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?

Please select:

A. Shutdown the instance
B. Remove the rule for incoming traffic on port 22 for the Security Group
C. Change the AMI for the instance
D. Change the Instance type for the instance

Answer: B

Explanation:
In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.
Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.
For more information on authorizing access to an instance, please visit the below URL: https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/authorizing-access-to-an-instance.htmll
The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

NEW QUESTION 92
- (Exam Topic 2)
A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.
The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.
How can the Security Engineer address the issue?

A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed
B. Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications
C. Use GuardDuty filters with auto archiving enabled to close the findings
D. Create an IAM Lambda function that closes the finding whenever a new occurrence is reported

Answer: B

Explanation:
Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your IAM infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per IAM account per region.

NEW QUESTION 93
- (Exam Topic 2)
Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.
Which of the following methods will ensure that the data is unreadable by anyone else?

A. Change the volume encryption on the EBS volume to use a different encryption mechanis
B. Then, release the EBS volumes back to IAM.
C. Release the volumes back to IA
D. IAM immediately wipes the disk after it is deprovisioned.
E. Delete the encryption key used to encrypt the EBS volum
F. Then, release the EBS volumes back to IAM.
G. Delete the data by using the operating system delete command
H. Run Quick Format on the drive and then release the EBS volumes back to IAM.

Answer: D

Explanation:
Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 (“Guidelines for Media Sanitization”), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements.
https://d0.IAMstatic.com/whitepapers/IAM-security-whitepaper.pdf

NEW QUESTION 96
- (Exam Topic 2)
The Security Engineer for a mobile game has to implement a method to authenticate users so that they can save their progress. Because most of the users are part of the same OpenID-Connect compatible social media website, the Security Engineer would like to use that as the identity provider.
Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

A. Amazon Cognito
B. AssumeRoleWithWebIdentity API
C. Amazon Cloud Directory
D. Active Directory (AD) Connector

Answer: A

NEW QUESTION 97
- (Exam Topic 2)
A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.

How can the security team fulfill these requirements?
Please select:

A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers.Redeploy all out of compliance instances/servers using an AMI with the latest patches.
B. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
C. Use Systems Manager Patch Manger to install the missing patches.
D. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers.Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
E. Use Trusted Advisor to generate the report of out of compliance instances/server
F. Use Systems Manger Patch Manger to install the missing patches.

Answer: B

Explanation:
Use the Systems Manger Patch Manger to generate the report and also install the missing patches The IAM Documentation mentions the following
IAM Systems Manager Patch Manager automates the process of patching managed instances with
security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.
Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers
Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.
For more information on the IAM Patch Manager, please visit the below URL: https://docs.IAM.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html (
The correct answer is: Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches.
Submit your Feedback/Queries to our Experts

NEW QUESTION 100
- (Exam Topic 2)
A Security Administrator is restricting the capabilities of company root user accounts. The company uses IAM Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational IAM resource purposes.
How can the Administrator restrict usage of member root user accounts across the organization?

A. Disable the use of the root user account at the organizational roo
B. Enable multi-factor authentication of the root user account for each organizational member account.
C. Configure IAM user policies to restrict root account capabilities for each Organizations member account.
D. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root use
E. Add all operational accounts to the new OU.
F. Configure IAM CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C

Explanation:
Applying a "Control Policy" in your organization. A policy applied to: 1) root applies to all accounts in the organization 2) OU applies to all accounts in the OU and to any child OUs 3) account applies to one account only Note- this requires that Acquirements: -all features are enabled for the organization in IAM Organizations -Only service control policy (SCP) are supported
https://docs.IAM.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

NEW QUESTION 104
- (Exam Topic 2)
For compliance reasons, an organization limits the use of resources to three specific IAM regions. It wants to be alerted when any resources are launched in unapproved regions.
Which of the following approaches will provide alerts on any resources launched in an unapproved region?

A. Develop an alerting mechanism based on processing IAM CloudTrail logs.
B. Monitor Amazon S3 Event Notifications for objects stored in buckets in unapproved regions.
C. Analyze Amazon CloudWatch Logs for activities in unapproved regions.
D. Use IAM Trusted Advisor to alert on all resources being created.

Answer: A

Explanation:
https://stackoverflow.com/questions/45449053/cloudwatch-alert-on-any-instance-creation

NEW QUESTION 109
- (Exam Topic 2)
A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.
Which solution would be MOST secure and easy to maintain?

A. Use IAM Certificate Manager to generate certificates from a public certificate authority and deploy them to all the containers.
B. Create a self-signed certificate in one container and use IAM Secrets Manager to distribute the certificate to the other containers to establish trust.
C. Use IAM Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then create the private keys in the containers and sign them using the ACM PCA API.
D. Use IAM Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then use IAM Certificate Manager to generate the private certificates and deploy them to all the containers.

Answer: D

NEW QUESTION 114
- (Exam Topic 2)
A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack? Please select:

A. Change the Inbound Security Groups to deny access from the suspecting IP
B. Change the Outbound Security Groups to deny access from the suspecting IP
C. Change the Inbound NACL to deny access from the suspecting IP
D. Change the Outbound NACL to deny access from the suspecting IP

Answer: C

Explanation:
Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.
Option D is invalid since just changing the Inbound Rules is sufficient The IAM Documentation mentions the following
A network access control list (ACLJ is an optional layer of security for your VPC that acts as a firewall for
controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.
The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

NEW QUESTION 115
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to IAM. They want to leverage their existing on-premises Active Directory as an identity provider for IAM.
Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with IAM? (Choose two.)

A. Create IAM roles with permissions corresponding to each Active Directory group.
B. Create IAM groups with permissions corresponding to each Active Directory group.
C. Configure Amazon Cloud Directory to support a SAML provider.
D. Configure Active Directory to add relying party trust between Active Directory and IAM.
E. Configure Amazon Cognito to add relying party trust between Active Directory and IAM.

Answer: AD

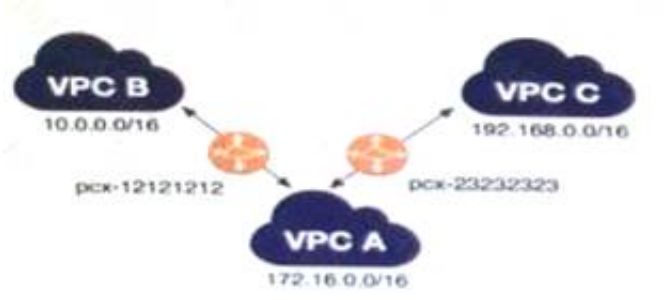
Explanation:
https://IAM.amazon.com/blogs/security/how-to-establish-federated-access-to-your-IAM-resources-by-using-acti

NEW QUESTION 116
- (Exam Topic 2)
What are the MOST secure ways to protect the IAM account root user of a recently opened IAM account? (Choose two.)

A. Use the IAM account root user access keys instead of the IAM Management Console
B. Enable multi-factor authentication for the IAM IAM users with the AdministratorAccess managed policy attached to them
C. Enable multi-factor authentication for the IAM account root user
D. Use IAM KMS to encrypt all IAM account root user and IAM IAM access keys and set automatic rotation to 30 days
E. Do not create access keys for the IAM account root user; instead, create IAM IAM users

Answer: CE

NEW QUESTION 117
- (Exam Topic 2)
A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.
How can this be accomplished? (Choose two.)



A. Deploy a pre-authorized scanning engine from the IAM Marketplace into VPC B, and use it to scan instances in all three VPC
B. Do not complete the penetration test request form.
C. Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VP
D. Do not complete the penetration test request form.
E. Create a VPN connection from the data center to VPC
F. Use an on-premises scanning engine to scan the instances in all three VPC
G. Complete the penetration test request form for all three VPCs.
H. Create a VPN connection from the data center to each of the three VPC
I. Use an on-premises scanning engine to scan the instances in each VP
J. Do not complete the penetration test request form.
K. Create a VPN connection from the data center to each of the three VPC
L. Use an on-premises scanning engine to scan the instances in each VP
M. Complete the penetration test request form for all three VPCs.

Answer: BD

Explanation:
https://IAM.amazon.com/security/penetration-testing/

NEW QUESTION 119
- (Exam Topic 2)
A company has contracted with a third party to audit several IAM accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

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

Answer: ACF

Explanation:
Using IAM to grant access to a Third-Party Account 1) Create a role to provide access to the require resources 1.1) Create a role policy that specifies the IAM Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition 1.2) Create a role using the role policy just created 1.3) Assign a resouce policy to the role. This will provide permission to access resource ARNs to the auditor 2) Repeat steps 1 and 2 on all IAM accounts 3) The auditor connects to the IAM account IAM Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3, sts:ExternalID 4) STS provide the auditor with temporary credentials that provides the role access from step 1
https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html
https://IAM.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-IAM-cloudtrail-and-amazon-clo

NEW QUESTION 122
- (Exam Topic 2)
A Security Administrator is performing a log analysis as a result of a suspected IAM account compromise. The Administrator wants to analyze suspicious IAM CloudTrail log files but is overwhelmed by the volume of audit logs being generated.
What approach enables the Administrator to search through the logs MOST efficiently?

A. Implement a “write-only” CloudTrail event filter to detect any modifications to the IAM account resources.
B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
D. Enable Amazon S3 event notifications to trigger an IAM Lambda function that sends an email alarm when there are new CloudTrail API entries.

Answer: C

NEW QUESTION 123
- (Exam Topic 2)
An application has been written that publishes custom metrics to Amazon CloudWatch. Recently, IAM changes have been made on the account and the metrics are no longer being reported.
Which of the following is the LEAST permissive solution that will allow the metrics to be delivered?

A. Add a statement to the IAM policy used by the application to allow logs:putLogEvents and logs:createLogStream
B. Modify the IAM role used by the application by adding the CloudWatchFullAccess managed policy.
C. Add a statement to the IAM policy used by the application to allow cloudwatch:putMetricData.
D. Add a trust relationship to the IAM role used by the application for cloudwatch.amazonIAM.com.

Answer: C

Explanation:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/monitoring/permissions-reference-cw.html

NEW QUESTION 128
- (Exam Topic 2)
A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.
How should the Lambda function be given access to the DynamoDB table? Please select:

A. Create a VPC endpoint for DynamoDB within a VP
B. Configure the Lambda function to access resources in the VPC.
C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table.Attach the poll to the DynamoDB table.
D. Create an IAM user with permissions to write to the DynamoDB tabl
E. Store an access key for that userin the Lambda environment variables.
F. Create an IAM service role with permissions to write to the DynamoDB tabl
G. Associate that role with the Lambda function.

Answer: D

Explanation:
The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function
The IAM Documentation additionally mentions the following
Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what IAM Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other IAM resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.
If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), IAM Lambda polls these streams on your behalf. IAM Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.
Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB
Option B is invalid because resources policies are present for resources such as S3 and KMS, but not IAM Lambda
Option C is invalid because IAM Roles should be used and not IAM Users
For more information on the Lambda permission model, please visit the below URL: https://docs.IAM.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.
Submit your Feedback/Queries to our Exp

NEW QUESTION 132
- (Exam Topic 2)
A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.
Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

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

Answer: CE

NEW QUESTION 135
- (Exam Topic 2)
A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:
-Content Security-Policy
-X-Frame-Options
-X-XSS-Protection
The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.
B. Implement an IAM Lambda@Edge origin response function that inserts the required headers.
C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.
D. Construct an IAM WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

Answer: B

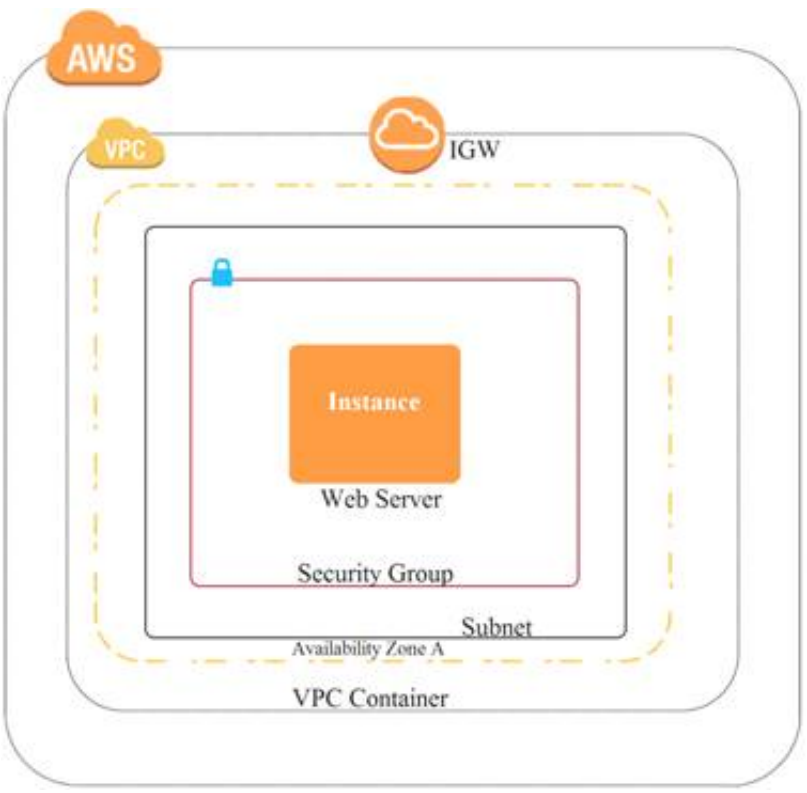
NEW QUESTION 139
- (Exam Topic 2)
During a security event, it is discovered that some Amazon EC2 instances have not been sending Amazon CloudWatch logs.
Which steps can the Security Engineer take to troubleshoot this issue? (Select two.)

A. Connect to the EC2 instances that are not sending the appropriate logs and verify that the CloudWatch Logs agent is running.
B. Log in to the IAM account and select CloudWatch Log
C. Check for any monitored EC2 instances that are in the “Alerting” state and restart them using the EC2 console.
D. Verify that the EC2 instances have a route to the public IAM API endpoints.
E. Connect to the EC2 instances that are not sending log
F. Use the command prompt to verify that the right permissions have been set for the Amazon SNS topic.
G. Verify that the network access control lists and security groups of the EC2 instances have the access to send logs over SNMP.

Answer: AC

Explanation:
https://docs.IAM.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-and-interface-VPC.html

NEW QUESTION 143
- (Exam Topic 2)
A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.
Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?



A. Move all the files to an Amazon S3 bucke
B. Have the web server serve the files from the S3 bucket.
C. Launch a second Amazon EC2 instance in a new subne
D. Launch an Application Load Balancer in front of both instances.
E. Launch an Application Load Balancer in front of the EC2 instanc
F. Create an Amazon CloudFront distribution in front of the Application Load Balancer.
G. Move all the files to an Amazon S3 bucke
H. Create a CloudFront distribution in front of the bucket and terminate the web server.

Answer: D

Explanation:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html

NEW QUESTION 144
- (Exam Topic 2)
An organization has a system in IAM that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes. A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks.
Which solution would remediate the audit finding while minimizing the effort required?

A. Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.
B. Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.
C. Use IAM Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service's servers.
D. Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

Answer: C

NEW QUESTION 148
- (Exam Topic 2)
Your company has a set of resources defined in the IAM Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?
Please select:

A. Create a powershell script using the IAM CL
B. Query for all resources with the tag of production.
C. Create a bash shell script with the IAM CL
D. Query for all resources in all region
E. Store the results in an S3 bucket.
F. Use Cloud Trail to get the list of all resources
G. Use IAM Config to get the list of all resources

Answer: D

Explanation:
The most feasible option is to use IAM Config. When you turn on IAM Config, you will get a list of resources defined in your IAM Account.
A sample snapshot of the resources dashboard in IAM Config is shown below C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.
Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on IAM Config, please visit the below URL: https://docs.IAM.amazon.com/config/latest/developereuide/how-does-confie-work.html
The correct answer is: Use IAM Config to get the list of all resources
Submit your Feedback/Queries to our Experts

NEW QUESTION 150
- (Exam Topic 2)
You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective
Please select:

A. Use a VPC endpoint
B. Attach an Internet gateway to the subnet
C. Attach a VPN connection to the VPC
D. Use VPC Peering

Answer: A

Explanation:
The IAM Documentation mentions the following
You can connect directly to IAM KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and IAM KMS is conducted entirely within the IAM network.
Option B is invalid because this could open threats from the internet
Option C is invalid because this is normally used for communication between on-premise environments and IAM.
Option D is invalid because this is normally used for communication between VPCs
For more information on accessing KMS via an endpoint, please visit the following URL https://docs.IAM.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.htmll
The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 152
- (Exam Topic 2)
A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted
with the same IAM KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.
The company's Developer Operations department learns about this only after the CMK has been deleted. Which steps must be taken to address this situation?

A. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.
C. Make a request to IAM Support to recover the S3 encrypted data.
D. Make a request to IAM Support to restore the deleted CMK, and use it to recover the data.

Answer: A

Explanation:
https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys.html#deleting-keys-how-it-works

NEW QUESTION 156
- (Exam Topic 2)
A Security Engineer who was reviewing IAM Key Management Service (IAM KMS) key policies found this statement in each key policy in the company IAM account.

```
{
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",
      "Resource": "*"
}
```

What does the statement allow?

A. All principals from all IAM accounts to use the key.
B. Only the root user from account 111122223333 to use the key.
C. All principals from account 111122223333 to use the key but only on Amazon S3.
D. Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

Answer: D

NEW QUESTION 158
- (Exam Topic 2)
A company runs an application on IAM that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.
How can the Security Engineer protect this workload so that only employees can access it?

A. Add each employee's home IP address to the security group for the application so that only those users can access the workload.
B. Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.
C. Use a VPN appliance from the IAM Marketplace for users to connect to, and restrict workload access to traffic from that appliance.
D. Route all traffic to the workload through IAM WA
E. Add each employee's home IP address into an IAM WAF rule, and block all other traffic.

Answer: C

Explanation:
https://docs.IAM.amazon.com/vpn/latest/clientvpn-admin/what-is.html

NEW QUESTION 159
- (Exam Topic 2)
An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.
Which steps should be taken to troubleshoot the issue? (Choose two.)

A. Use an EC2 run command to confirm that the "IAMlogs" service is running on all instances.
B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
C. Check whether any application log entries were rejected because of invalid time stamps by reviewing/var/cwlogs/rejects.log.
D. Check that the trust relationship grants the service "cwlogs.amazonIAM.com" permission to write objects to the Amazon S3 staging bucket.
E. Verify that the time zone on the application servers is in UTC.

Answer: AB

Explanation:
EC2 run command - can run scripts, install software, collect metrics and log files, manage patches and more. Bringing these two services together - can create CloudWatch Events rules that use EC2 Run Command to perform actions on EC2 instances or on-premises servers.

NEW QUESTION 164
- (Exam Topic 2)
Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?
Please select:

A. Use IAM Inspector to inspect all the security Groups
B. Use the IAM Trusted Advisor to see which security groups have compromised access.
C. Use IAM Config to see which security groups have compromised access.
D. Use the IAM CLI to query the security groups and then filter for the rules which have unrestricted accessd

Answer: B

Explanation:
The IAM Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).
If you go to IAM Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is invalid because IAM Inspector is used to detect security vulnerabilities in instances and not for security groups.
Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.
Option Dis partially valid but would just be a maintenance overhead
For more information on the IAM Trusted Advisor, please visit the below URL: https://IAM.amazon.com/premiumsupport/trustedadvisor/best-practices;
The correct answer is: Use the IAM Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 165
- (Exam Topic 2)
An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.
Which steps should be taken to investigate the suspected compromise? (Choose three.)

A. Detach the elastic network interface from the EC2 instance.
B. Initiate an Amazon Elastic Block Store volume snapshot of all volumes on the EC2 instance.
C. Disable any Amazon Route 53 health checks associated with the EC2 instance.
D. De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.
E. Attach a security group that has restrictive ingress and egress rules to the EC2 instance.
F. Add a rule to an IAM WAF to block access to the EC2 instance.

Answer: BDE

Explanation:
https://d1.IAMstatic.com/whitepapers/IAM_security_incident_response.pdf

NEW QUESTION 168
- (Exam Topic 2)
You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

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

```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
     "s3:ListAllMyBuckets",
     "s3:GetBucketLocation"
 ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
  "Bool": {"aws:MultiFactorAuthPresent": true}
 }
}
}
```

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

```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
     "s3:ListAllMyBuckets",
     "s3:GetBucketLocation"
 ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
  "Bool": {"aws:MultiFactorAuthPresent":false}
 }
}
```

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

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

Answer: A

Explanation:
The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated. Option B and C are wrong since the IAM:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.
Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to
"true" or "false."
Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.
For more information on an example on such a policy, please visit the following URL:

NEW QUESTION 172
- (Exam Topic 2)
A Development team has asked for help configuring the IAM roles and policies in a new IAM account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).
Which of the following will allow the team to manage IAM KMS permissions in IAM without the complexity of editing individual key policies?

A. The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.
B. Newly created CMKs must have a key policy that allows the root principal to perform all actions.
C. Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
D. Newly created CMKs must mirror the IAM policy of the KMS key administrator.

Answer: B

Explanation:
https://docs.IAM.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enabl

NEW QUESTION 177
- (Exam Topic 2)
A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user's IAM permissions in the case of a security incident.
How can this be accomplished?

A. Use IAM Config to review the IAM policy assigned to users before and after the incident.
B. Run the GenerateCredentialReport via the IAM CLI, and copy the output to Amazon S3 daily for auditing purposes.
C. Copy IAM CloudFormation templates to S3, and audit for changes from the template.
D. Use Amazon EC2 Systems Manager to deploy images, and review IAM CloudTrail logs for changes.

Answer: A

Explanation:
https://IAM.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-IAM

NEW QUESTION 180
- (Exam Topic 2)
An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.

Which of the following supports this requirement for IAM resources that are encrypted by IAM KMS?

A. Copy the application's IAM KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.
B. Configure IAM KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
C. Use IAM services that replicate data across regions, and re-wrap the data encryption key created in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.
D. Configure the target region's IAM service to communicate with the source region's IAM KMS so that it can decrypt the resource in the target region.

Answer: C

NEW QUESTION 181
- (Exam Topic 2)
A Developer who is following IAM best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using IAM KMS. What is the simplest and MOST secure way to decrypt this data when required?

A. Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.
B. Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policie
C. Query DynamoDB to retrieve the data key to decrypt the data
D. Use the Encrypt API to store an encrypted version of the data key with another customer managed key.Decrypt the data key and use it to decrypt the data when required.
E. Store the encrypted data key alongside the encrypted dat
F. Use the Decrypt API to retrieve the data key to decrypt the data when required.

Answer: D

Explanation:
We recommend that you use the following pattern to locally encrypt data: call the GenerateDataKey API, use the key returned in the Plaintext response field to locally encrypt data, and then erase the plaintext data key from memory. Store the encrypted data key (contained in the CiphertextBlob field) alongside of the locally encrypted data. The Decrypt API returns the plaintext key from the encrypted key.
https://docs.IAM.amazon.com/sdkfornet/latest/apidocs/items/MKeyManagementServiceKeyManagementServic

NEW QUESTION 183
- (Exam Topic 2)
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target IAM account (123456789123) to perform their job functions.
A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

What should be done to enable the user to assume the appropriate role in the target account?

A Update the IAM policy attached to the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::123456789123:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

B Update the trust policy on the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::987654321987:role/IdentityRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

C Update the trust policy on the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::987654321987:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

D Update the IAM policy attached to the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1502946463000",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::123456789123:role/JobFunctionRole"
        }
    ]
}
```

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

Answer: A

NEW QUESTION 185
- (Exam Topic 2)
A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:
- Encryption in transit
- Encryption at rest
- Logging of all object retrievals in IAM CloudTrail

Which of the following meet these security requirements? (Choose three.)

A. Specify “IAM:SecureTransport”: “true” within a condition in the S3 bucket policy.
B. Enable a security group for the S3 bucket that allows port 443, but not port 80.
C. Set up default encryption for the S3 bucket.
D. Enable Amazon CloudWatch Logs for the IAM account.
E. Enable API logging of data events for all S3 objects.
F. Enable S3 object versioning for the S3 bucket.

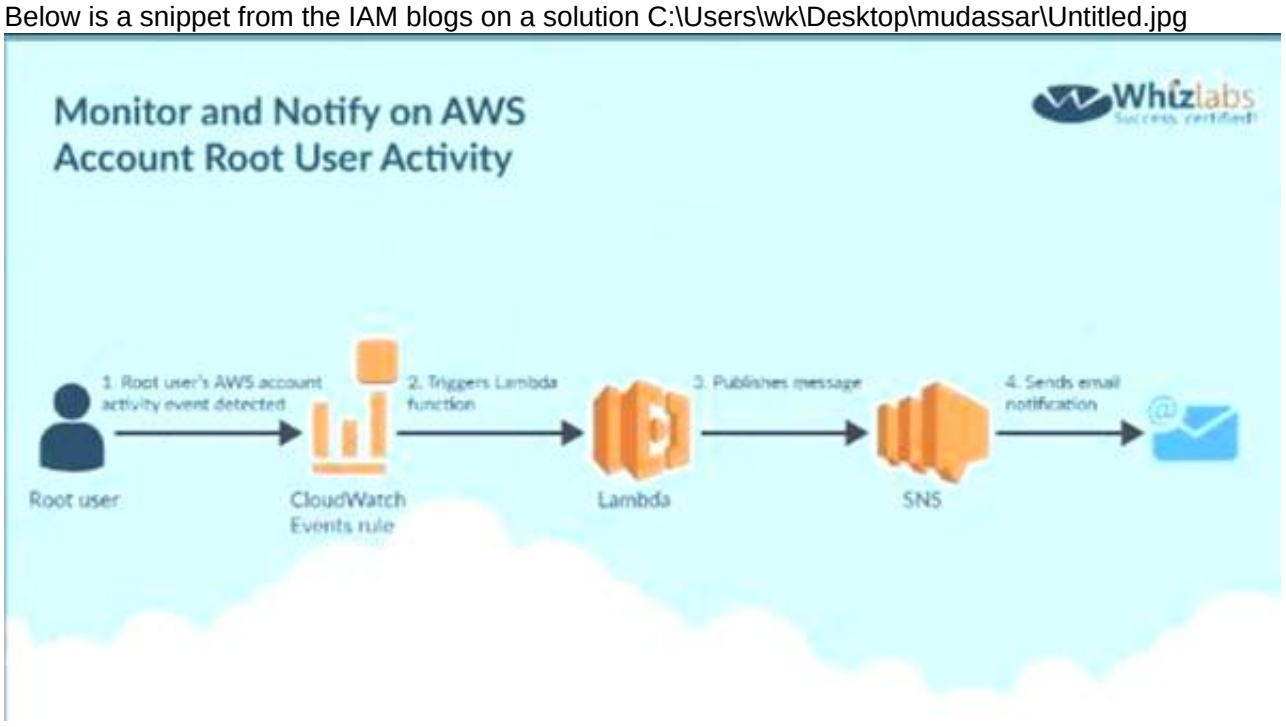
Answer: ACE

NEW QUESTION 188
- (Exam Topic 2)
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

A. Create a Cloudwatch Events Rule s
B. Create a Cloudwatch Logs Rule
C. Use a Lambda function
D. Use Cloudtrail API call

Answer: AC

Explanation:
Below is a snippet from the IAM blogs on a solution C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:
https://IAM.amazon.com/blogs/mt/monitor-and-notify-on-IAM-account-root-user-activityy The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function
Submit your Feedback/Queries to our Experts

NEW QUESTION 193
- (Exam Topic 2)
A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by IAM Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.
After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.
B. Enabling rotation in Secrets Manager causes the secret to rotate immediately, and the applications are using the earlier credential.
C. The Secrets Manager IAM policy does not allow access to the RDS database.
D. The Secrets Manager IAM policy does not allow access for the applications.

Answer: B

Explanation:
https://docs.IAM.amazon.com/secretsmanager/latest/userguide/enable-rotation-rds.html

NEW QUESTION 198
- (Exam Topic 2)
You have a 2 tier application hosted in IAM. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.
Please select:

A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0
B. db-345 - Allow port 1433 from wg-123
C. wg-123 - Allow port 1433 from wg-123
D. db-345 -Allow ports 1433 from 0.0.0.0/0

Answer: AB

Explanation:
The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.
The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-security.htmll
The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123
Submit your Feedback/Queries to our Experts

NEW QUESTION 200
- (Exam Topic 2)
An application makes calls to IAM services using the IAM SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.
Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

A. Confirm that the EC2 instance's security group authorizes S3 access.
B. Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.
C. Check the S3 bucket policy for statements that deny access to objects.
D. Confirm that the EC2 instance is using the correct key pair.

E. Confirm that the IAM role associated with the EC2 instance has the proper privileges.
F. Confirm that the instance and the S3 bucket are in the same Region.

Answer: BCE

NEW QUESTION 204
- (Exam Topic 2)
Which approach will generate automated security alerts should too many unauthorized IAM API requests be identified?

A. Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric's rate.
B. Configure IAM CloudTrail to stream event data to Amazon Kinesi
C. Configure an IAM Lambda function on the stream to alarm when the threshold has been exceeded.
D. Run an Amazon Athena SQL query against CloudTrail log file
E. Use Amazon QuickSight to create an operational dashboard.
F. Use the Amazon Personal Health Dashboard to monitor the account's use of IAM services, and raise an alert if service error rates increase.

Answer: A

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatc Open the CloudWatch console at https://console.IAM.amazon.com/cloudwatch/. In the navigation pane,
choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") } Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

NEW QUESTION 206
- (Exam Topic 2)
A security team is responsible for reviewing IAM API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future IAM regions.
What is the SIMPLEST way to meet these requirements?

A. Enable IAM Trusted Advisor security checks in the IAM Console, and report all security incidents for all regions.
B. Enable IAM CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
C. Enable IAM CloudTrail by creating a new trail and applying the trail to all region
D. Specify a single Amazon S3 bucket as the storage location.
E. Enable Amazon CloudWatch logging for all IAM services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer: C

Explanation:
https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/creating-trail-organization.html

NEW QUESTION 207
- (Exam Topic 2)
The IAM Systems Manager Parameter Store is being used to store database passwords used by an IAM Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an IAM KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.
Which of the following actions will resolve the access denied error?

A. Update the ssm.amazonIAM.com principal in the KMS key policy to allow kms: Decrypt.
B. Update the Lambda configuration to launch the function in a VPC.
C. Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
D. Add lambda.amazonIAM.com as a trusted entity on the IAM role that the Lambda function uses.

Answer: C

Explanation:
https://docs.amazonIAM.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Authorizin

NEW QUESTION 211
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to IAM. The company wants to leverage its existing on-premises Active Directory as an identity provider for IAM.
Which steps should be taken to authenticate to IAM services using the company's on-premises Active Directory? (Choose three).

A. Create IAM roles with permissions corresponding to each Active Directory group.
B. Create IAM groups with permissions corresponding to each Active Directory group.
C. Create a SAML provider with IAM.
D. Create a SAML provider with Amazon Cloud Directory.
E. Configure IAM as a trusted relying party for the Active Directory
F. Configure IAM as a trusted relying party for Amazon Cloud Directory.

Answer: ACE

Explanation:
https://IAM.amazon.com/blogs/security/IAM-federated-authentication-with-active-directory-federation-services

NEW QUESTION 213
- (Exam Topic 2)
A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).
What mechanism will allow the company to implement all required network rules without incurring additional cost?

A. Configure IAM WAF rules to implement the required rules.
B. Use the operating system built-in, host-based firewall to implement the required rules.
C. Use a NAT gateway to control ingress and egress according to the requirements.
D. Launch an EC2-based firewall product from the IAM Marketplace, and implement the required rules in that product.

Answer: B

NEW QUESTION 215
- (Exam Topic 2)
A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below
Please select:

A. Port 443 coming from 0.0.0.0/0
B. Port 443 coming from 10.0.0.0/16
C. Port 22 coming from 0.0.0.0/0
D. Port 22 coming from 203.0.113.1/32

Answer: AD

Explanation:
Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.
Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk
For more information on IAM Security Groups, please visit the following UR
https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/usins-network-secunty.htmll
The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

NEW QUESTION 219
- (Exam Topic 2)
A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year.
What can be done to implement the above policy?

A. Enable automatic key rotation annually for the CMK.
B. Use IAM Command Line Interface to create an IAM Lambda function to rotate the existing CMK annually.
C. Import new key material to the existing CMK and manually rotate the CMK.
D. Create a new CMK, import new key material to it, and point the key alias to the new CMK.

Answer: D

Explanation:
https://docs.IAM.amazon.com/en_pv/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually "You might prefer to rotate keys manually so you can control the rotation frequency. It's also a good solution
for CMKs that are not eligible for automatic key rotation, such as asymmetric CMKs, CMKs in custom key stores and CMKs with imported key material. Because the new CMK is a different resource from the current CMK, it has a different key ID and ARN. When you change CMKs, you need to update references to the CMK ID or ARN in your applications. Aliases, which associate a friendly name with a CMK, make this process easier. Use an alias to refer to a CMK in your applications. Then, when you want to change the CMK that the application uses, change the target CMK of the alias. To update the target CMK of an alias, use UpdateAlias operation in the IAM KMS API. "

NEW QUESTION 223
- (Exam Topic 2)
The Security team believes that a former employee may have gained unauthorized access to IAM resources sometime in the past 3 months by using an identified access key.
What approach would enable the Security team to find out what the former employee may have done within IAM?

A. Use the IAM CloudTrail console to search for user activity.
B. Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.
C. Use IAM Config to see what actions were taken by the user.
D. Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

Answer: A

Explanation:
You can use CloudTrail to search event history for the last 90 days. You can use CloudWatch queries to search API history beyond the last 90 days. You can use Athena to query CloudTrail logs over the last 90 days. https://IAM.amazon.com/premiumsupport/knowledge-center/view-iam-history/

NEW QUESTION 228
- (Exam Topic 2)
A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification.
What is the MOST efficient way to meet these requirements?

A. Install antivirus software and ensure that signatures are up-to-dat
B. Configure Amazon CloudWatch alarms to send alerts for security events.
C. Install host-based IDS software to check for file integrit
D. Export the logs to Amazon CloudWatch Logs for monitoring and alerting.
E. Export system log files to Amazon S3. Parse the log files using an IAM Lambda function that will send alerts of any unauthorized system login attempts through Amazon SNS.
F. Use Amazon CloudWatch Logs to detect file system change
G. If a change is detected, automaticallyterminate and recreate the instance from the most recent AM
H. Use Amazon SNS to send notification of the event.

Answer: B

NEW QUESTION 231
- (Exam Topic 2)
Your company is planning on hosting an internal network in IAM. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.
Please select:

A. Consider using Windows Server 2016 Certificate Manager
B. Consider using IAM Certificate Manager
C. Consider using IAM Access keys to generate the certificates
D. Consider using IAM Trusted Advisor for managing the certificates

Answer: B

Explanation:
The IAM Documentation mentions the following
ACM is tightly linked with IAM Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted
Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", IAM Certificate Manager should be used
Option C and D are invalid because these cannot be used for managing certificates. For more information on ACM, please visit the below URL: https://docs.IAM.amazon.com/acm/latest/userguide/acm-overview.html
The correct answer is: Consider using IAM Certificate Manager Submit your Feedback/Queries to our Experts

NEW QUESTION 235
- (Exam Topic 3)
An auditor needs access to logs that record all API events on IAM. The auditor only needs read-only access to the log files and does not need access to each IAM account. The company has multiple IAM accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below
Please select:

A. Configure the CloudTrail service in each IAM account, and have the logs delivered to an IAM bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary IAM account that can assume a read-only role in the secondary IAM accounts.
B. Configure the CloudTrail service in the primary IAM account and configure consolidated billing for all the secondary account
C. Then grant the auditor access to the S3 bucket that receives the CloudTrail log files.
D. Configure the CloudTrail service in each IAM account and enable consolidated logging inside of CloudTrail.
E. Configure the CloudTrail service in each IAM account and have the logs delivered to a single IAM bucket in the primary account and erant the auditor access to that single bucket in the orimarv account.

Answer: D

Explanation:
Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of IAM resources as possibli
IAM CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your IAM account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your IAM infrastructure. CloudTrail provides a history of IAM API calls for your account including API calls made through the IAM Management Console, IAM SDKs, command line tools, and other IAM services. This history simplifies security analysis, resource change tracking, and troubleshooting
only be granted access in one location
Option Option A is incorrect since the auditor should B is incorrect since consolidated billing is not a key
requirement as part of the question
Option C is incorrect since there is not consolidated logging
For more information on Cloudtrail please refer to the below URL: https://IAM.amazon.com/cloudtraiL
(
The correct answer is: Configure the CloudTrail service in each IAM account and have the logs delivered to a single IAM bud in the primary account and grant the auditor access to that single bucket in the primary account.
Submit your Feedback/Queries to our Experts

NEW QUESTION 237
- (Exam Topic 3)
Your company has the following setup in IAM
* a. A set of EC2 Instances hosting a web application
* b. An application load balancer placed in front of the EC2 Instances
There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests?
Please select:

A. Use Security Groups to block the IP addresses
B. Use VPC Flow Logs to block the IP addresses

C. Use IAM inspector to block the IP addresses
D. Use IAM WAF to block the IP addresses

Answer: D

Explanation:
Your answer is incorrect Answer -D
The IAM Documentation mentions the following on IAM WAF which can be used to protect Application Load Balancers and Cloud front
A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:
Originate from an IP address or a range of IP addresses Originate from a specific country or countries
Contain a specified string or match a regular expression (regex) pattern in a particular part of requests Exceed a specified length
Appear to contain malicious SQL code (known as SQL injection) Appear to contain malicious scripts (known as cross-site scripting)
Option A is invalid because by default Security Groups have the Deny policy
Options B and C are invalid because these services cannot be used to block IP addresses For information on IAM WAF, please visit the below URL: https://docs.IAM.amazon.com/waf/latest/developerguide/web-acl.html
The correct answer is: Use IAM WAF to block the IP addresses Submit your Feedback/Queries to our Experts

NEW QUESTION 239
- (Exam Topic 3)
You have a set of Keys defined using the IAM KMS service. You want to stop using a couple of keys , but are not sure of which services are currently using the keys. Which of the following would be a safe option to stop using the keys from further usage.
Please select:

A. Delete the keys since anyway there is a 7 day waiting period before deletion
B. Disable the keys
C. Set an alias for the key
D. Change the key material for the key

Answer: B

Explanation:
Option A is invalid because once you schedule the deletion and waiting period ends, you cannot come back from the deletion process.
Option C and D are invalid because these will not check to see if the keys are being used or not The IAM Documentation mentions the following
Deleting a customer master key (CMK) in IAM Key Management Service (IAM KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.
For more information on deleting keys from KMS, please visit the below URL: https://docs.IAM.amazon.com/kms/latest/developereuide/deleting-keys.html
The correct answer is: Disable the keys Submit your Feedback/Queries to our Experts

NEW QUESTION 244
- (Exam Topic 3)
Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service
Please select:

A. The master keys encrypts the cluster ke
B. The cluster key encrypts the database ke
C. The database key encrypts the data encryption keys.
D. The master keys encrypts the database ke
E. The database key encrypts the data encryption keys.
F. The master keys encrypts the data encryption key
G. The data encryption keys encrypts the database key
H. The master keys encrypts the cluster key, database key and data encryption keys

Answer: A

Explanation:
This is mentioned in the IAM Documentation
Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.
Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly-generated AES-256 key. These keys are encrypted by using the database key for the cluster.
The database key encrypts data encryption keys in the cluster. The database key is a randomly-generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.
The cluster key encrypts the database key for the Amazon Redshift cluster.
Option B is incorrect because the master key encrypts the cluster key and not the database key
Option C is incorrect because the master key encrypts the cluster key and not the data encryption keys Option D is incorrect because the master key encrypts the cluster key only
For more information on how keys are used in Redshift, please visit the following URL: https://docs.IAM.amazon.com/kms/latest/developereuide/services-redshift.html
The correct answer is: The master keys encrypts the cluster key. The cluster key encrypts the database key. The database key encrypts the data encryption keys.
Submit your Feedback/Queries to our Experts

NEW QUESTION 245
- (Exam Topic 3)
A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?
Please select:

A. Use Bucket policies

B. Use the Secure Token service
C. Use IAM user policies
D. Use IAM Access Keys

Answer: AC

Explanation:
The IAM Documentation mentions the following
Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.
Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below Link: https://docs.IAM.amazon.com/AmazonS3/latest/dev/s3-access-control.htmll
The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

NEW QUESTION 247
- (Exam Topic 3)
Your application currently uses customer keys which are generated via IAM KMS in the US east region. You now want to use the same set of keys from the EU-Central region. How can this be accomplished?
Please select:

A. Export the key from the US east region and import them into the EU-Central region
B. Use key rotation and rotate the existing keys to the EU-Central region
C. Use the backing key from the US east region and use it in the EU-Central region
D. This is not possible since keys from KMS are region specific

Answer: D

Explanation:
Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys
Option C is invalid because the backing key cannot be used to export keys This is mentioned in the IAM documentation
What geographic region are my keys stored in?
Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region
For more information on KMS please visit the following URL: https://IAM.amazon.com/kms/faqs/
The correct answer is: This is not possible since keys from KMS are region specific Submit your Feedback/Queries to our Experts

NEW QUESTION 248
- (Exam Topic 3)
A company has a set of EC2 instances hosted in IAM. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required.
Please select:

A. Use lifecycle policies for the EBS volumes
B. Use EBS Snapshots
C. Use EBS volume replication
D. Use EBS volume encryption

Answer: CD

Explanation:
Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability.
You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes.
With lifecycle management, you can be sure that snapshots are cleaned up regularly and keep costs under control.
EBS Lifecycle Policies
A lifecycle policy consists of these core settings:
• Resource type—The IAM resource managed by the policy, in this case, EBS volumes.
• Target tag—The tag that must be associated with an EBS volume for it to be managed by the policy.
• Schedule—Defines how often to create snapshots and the maximum number of snapshots to keep. Snapshot creation starts within an hour of the specified start time. If creating a new snapshot exceeds the maximum number of snapshots to keep for the volume, the oldest snapshot is deleted.
Option C is correct. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. But it does not have an explicit feature like that.
Option D is correct Encryption does not ensure data durability
For information on security for Compute Resources, please visit the below URL https://d1.IAMstatic.com/whitepapers/Security/Security Compute Services Whitepaper.pdl
The correct answers are: Use EBS volume replication. Use EBS volume encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 249
- (Exam Topic 3)
You are working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security?
Please select:

A. Save the API credentials to your PHP files.
B. Don't save your API credentials, instead create a role in IAM and assign this role to an EC2 instance when you first create it.

C. Save your API credentials in a public Github repository.
D. Pass API credentials to the instance using instance userdata.

Answer: B

Explanation:
Applications must sign their API requests with IAM credentials. Therefore, if you are an application
developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your IAM credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance. especially those that IAM creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your IAM credentials.
IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you manage the security credentials that the applications use.
Option A.C and D are invalid because using IAM Credentials in an application in production is a direct no recommendation 1 secure access
For more information on IAM Roles, please visit the below URL:
http://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html
The correct answer is: Don't save your API credentials. Instead create a role in IAM and assign this role to an EC2 instance when you first create it
Submit your Feedback/Queries to our Experts

NEW QUESTION 250
- (Exam Topic 3)
An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.
Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below
Please select:
A. A network ACL with a rule that allows outgoing traffic on port 443.
B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
D. A security group with a rule that allows outgoing traffic on port 443
E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports.
F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Answer: BD

Explanation:
Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port.
Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports
Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not
required
For more information on VPC Security Groups, please visit the below URL:
https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.htmll
The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443
Submit your Feedback/Queries to our Experts

NEW QUESTION 253
- (Exam Topic 3)
You need to ensure that the cloudtrail logs which are being delivered in your IAM account is encrypted. How can this be achieved in the easiest way possible?
Please select:

A. Don't do anything since CloudTrail logs are automatically encrypted.
B. Enable S3-SSE for the underlying bucket which receives the log files
C. Enable S3-KMS for the underlying bucket which receives the log files
D. Enable KMS encryption for the logs which are sent to Cloudwatch

Answer: A

Explanation:
The IAM Documentation mentions the following
By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3)
Option B,C and D are all invalid because by default all logs are encrypted when they sent by Cloudtrail to S3 buckets
For more information on IAM Cloudtrail log encryption, please visit the following URL: https://docs.IAM.amazon.com/IAMcloudtrail/latest/usereuide/encryptine-cloudtrail-loe-files-with-IAM-kms.htm The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your Feedback/Queries to our Experts

NEW QUESTION 257
- (Exam Topic 3)
Your company has many IAM accounts defined and all are managed via IAM Organizations. One IAM account has a S3 bucket that has critical data. How can we ensure that all the users in the IAM organisation have access to this bucket?
Please select:

A. Ensure the bucket policy has a condition which involves IAM:PrincipalOrgID
B. Ensure the bucket policy has a condition which involves IAM:AccountNumber
C. Ensure the bucket policy has a condition which involves IAM:PrincipaliD
D. Ensure the bucket policy has a condition which involves IAM:OrgID

Answer: A

Explanation:
The IAM Documentation mentions the following
IAM Identity and Access Management (IAM) now makes it easier for you to control access to your IAM resources by using the IAM organization of IAM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, IAM:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization
Option B.C and D are invalid because the condition in the bucket policy has to mention IAM:PrincipalOrgID For more information on controlling access via Organizations, please refer to the below Link:
https://IAM.amazon.com/blogs/security/control-access-to-IAM-resources-by-usins-the-IAM-organization-of-iam (
The correct answer is: Ensure the bucket policy has a condition which involves IAM:PrincipalOrgID Submit your Feedback/Queries to our Experts

NEW QUESTION 260
- (Exam Topic 3)
A company has been using the IAM KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below
Please select:

A. Determine the age of the master key
B. See who is assigned permissions to the master key
C. See Cloudtrail for usage of the key
D. Use IAM cloudwatch events for events generated for the key

Answer: BC

Explanation:
The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs
Option A is invalid because seeing how long ago the key was created would not determine the usage of the key
Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the IAM Documentation
Examining CMK Permissions to Determine the Scope of Potential Usage
Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an IAM KMS Customer Master Key.
Examining IAM CloudTrail Logs to Determine Actual Usage
IAM KMS is integrated with IAM CloudTrail, so all IAM KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all IAM KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it
For more information on determining the usage of CMK keys, please visit the following URL:
> https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html
The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

NEW QUESTION 261
- (Exam Topic 3)
A customer has an instance hosted in the IAM Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.
Please select:

A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator'sWorkstation
B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
C. Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
D. Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

Answer: C

Explanation:
Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.
The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.
Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originate' , from the IT admin's workstation.
The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

NEW QUESTION 264
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SCS-C02 Exam with Our Prep Materials Via below:

https://www.certleader.com/SCS-C02-dumps.html