Amazon-Web-Services

Exam Questions SCS-C01

AWS Certified Security- Specialty

NEW QUESTION 1
- (Exam Topic 1)
A Security Engineer has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.
The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a requirement that traffic between the web servers and the internet flow through the virtual security appliance.
The Security Engineer has verified the following:
* 1. The rule set in the Security Groups is correct
* 2. The rule set in the network ACLs is correct
* 3. The rule set in the virtual appliance is correct
Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)

A. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.
B. Verify which Security Group is applied to the particular web server’s elastic network interface (ENI).
C. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.
D. Verify the registered targets in the ALB.
E. Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

Answer: CD

Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

NEW QUESTION 2
- (Exam Topic 1)
A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on AWS, but does have AWS Systems Manager configured. The solution must also minimize administrative overhead.
What should a security engineer recommend to meet these requirements?

A. Create an AWS Config rule defining the patch as a required configuration for EC2 instances.
B. Use the AWS Systems Manager Run Command to patch affected instances.
C. Use an AWS Systems Manager Patch Manager predefined baseline to patch affected instances.
D. Use AWS Systems Manager Session Manager to log in to each affected instance and apply the patch.

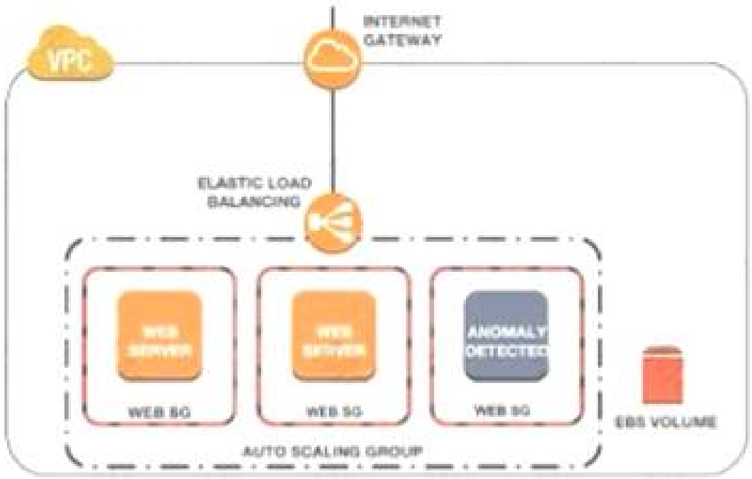
Answer: B

NEW QUESTION 3
- (Exam Topic 1)
A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:
• A trusted forensic environment must be provisioned
• Automated response processes must be orchestrated
Which AWS services should be included in the plan? {Select TWO)

A. AWS CloudFormation
B. Amazon GuardDuty
C. Amazon Inspector
D. Amazon Macie
E. AWS Step Functions

Answer: AE

NEW QUESTION 4
- (Exam Topic 1)
A Security Engineer noticed an anomaly within a company EC2 instance as shown in the image. The Engineer must now investigate what e causing the anomaly.
What are the MOST effective steps to take lo ensure that the instance is not further manipulated while allowing the Engineer to understand what happened?



A. Remove the instance from the Auto Scaling group Place the instance within an isolation security group, detach the EBS volume launch an EC2 instance with a forensic toolkit and attach the E8S volume to investigate
B. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, launch an EC2 instance

with a forensic toolkit, and allow the forensic toolkit image to connect to the suspicious Instance to perform the Investigation.
C. Remove the instance from the Auto Scaling group Place the Instance within an isolation security group, launch an EC2 Instance with a forensic toolkit and use the forensic toolkit imago to deploy an ENI as a network span port to inspect all traffic coming from the suspicious instance.
D. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, make a copy of the EBS volume from a new snapshot, launch an EC2 Instance with a forensic toolkit and attach the copy of the EBS volume to investigate.

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances wilt be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:
• Set up the proxy software on the EC2 instances.
• Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.
• Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.
However, the proxy EC2 instances are not successfully forwarding traffic to the internet.
What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

A. Put all the proxy EC2 instances in a cluster placement group.
B. Disable source and destination checks on the proxy EC2 instances.
C. Open all inbound ports on the proxy EC2 instance security group.
D. Change the VPC's DHCP domain-name-servers options set to the IP addresses of proxy EC2 instances.

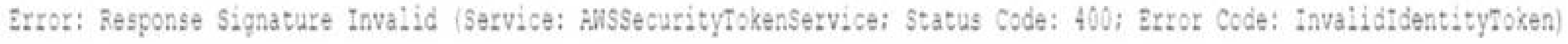
Answer: B

NEW QUESTION 6
- (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 AWS Key Management Service (AWS KMS) AWS 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 AWS Key Management Service (AWS KMS) AWS 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 AWS Key Management Service (AWS 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 AWS Key Management Service (AWS 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 7
- (Exam Topic 1)
A company uses a third-party identity provider and SAML-based SSO for its AWS accounts After the third-party identity provider renewed an expired signing certificate users saw the following message when trying to log in:



```
Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)
```

A security engineer needs to provide a solution that corrects the error and minimizes operational overhead Which solution meets these requirements?

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

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
A security engineer must develop an encryption tool for a company. The company requires a cryptographic solution that supports the ability to perform cryptographic erasure on all resources protected by the key material in 15 minutes or less
Which AWS Key Management Service (AWS KMS) key solution will allow the security engineer to meet these requirements?

A. Use Imported key material with CMK
B. Use an AWS KMS CMK
C. Use an AWS managed CMK.
D. Use an AWS KMS customer managed CMK

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
A company has multiple production AWS accounts. Each account has AWS CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.
Which steps should be taken to troubleshoot the issue? (Choose three.)

A. Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.
B. Verify that the S3 bucket policy allows access for CloudTrail from the production AWS account IDs.
C. Create a new CloudTrail configuration in the account, and configure it to log to the account's S3 bucket.
D. Confirm in the CloudTrail Console that each trail is active and healthy.
E. Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.
F. Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

Answer: BDF

NEW QUESTION 10
- (Exam Topic 1)
A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application
Which combination of actions would provide the MOST secure solution? (Select TWO)

A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances
B. Enable AWS WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances
C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs
D. Create a usage plan Generate a set of API keys for each application that needs to call the API.
E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

Answer: AE

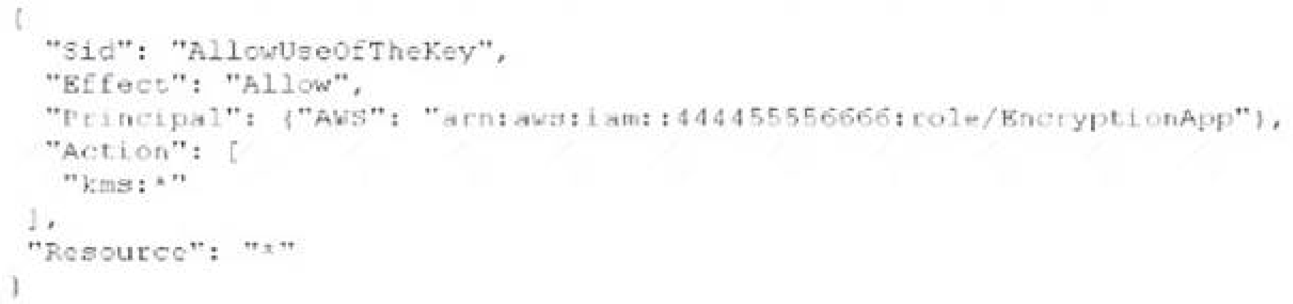
NEW QUESTION 10
- (Exam Topic 1)
A company uses Microsoft Active Directory for access management for on-premises resources and wants to use the same mechanism for accessing its AWS accounts. Additionally, the development team plans to launch a public-facing application for which they need a separate 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 AWS
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 AWS through ADFS and SAML.

Answer: CD

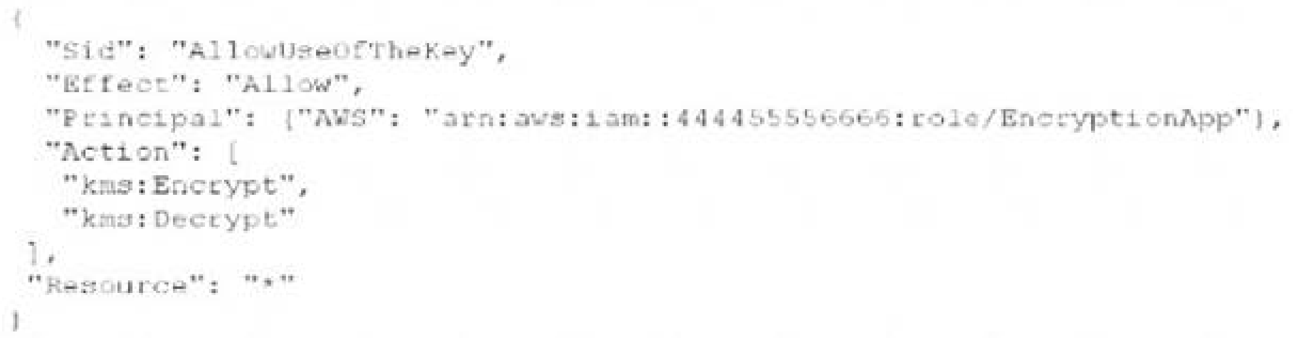
NEW QUESTION 12
- (Exam Topic 1)
An application developer is using an AWS Lambda function that must use AWS KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB Which key policy would allow the application to do this while granting least privilege?

A.



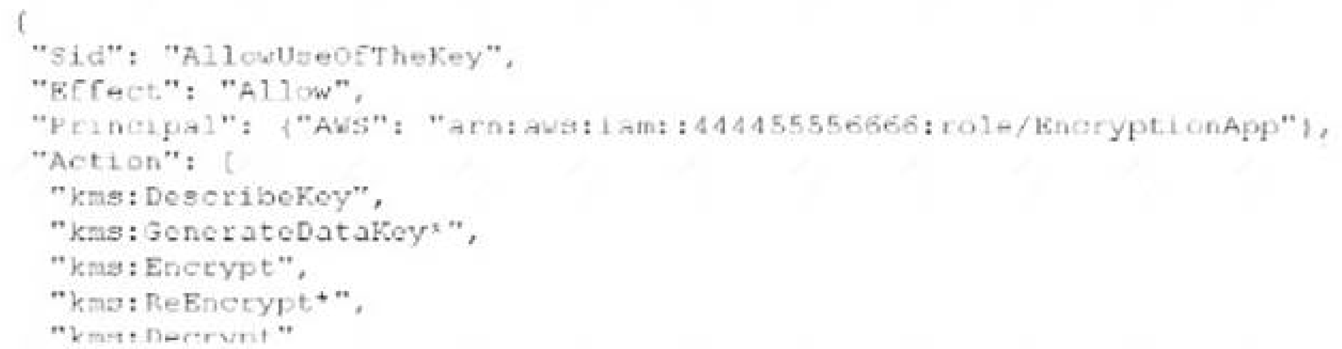
```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
   "kms:*"
 ],
 "Resource": "*"
}
```

B.



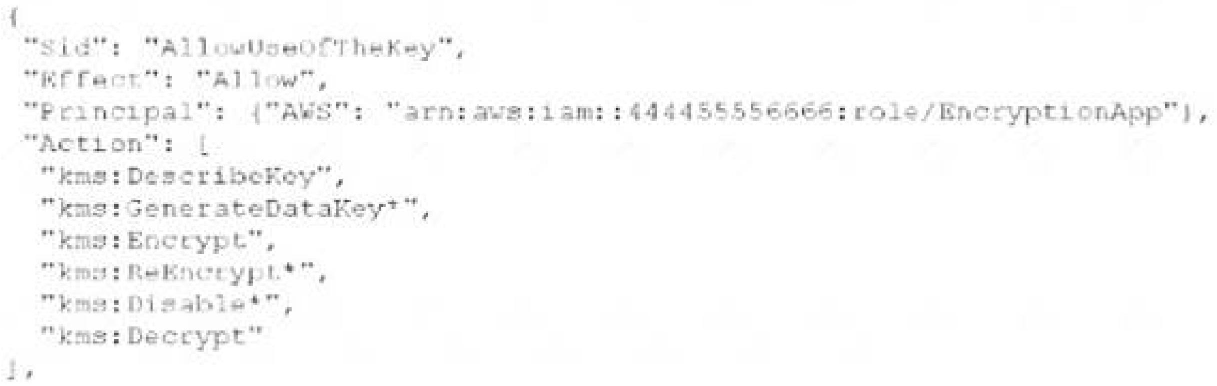
```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
   "kms:Encrypt",
   "kms:Decrypt"
 ],
 "Resource": "*"
}
```

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.



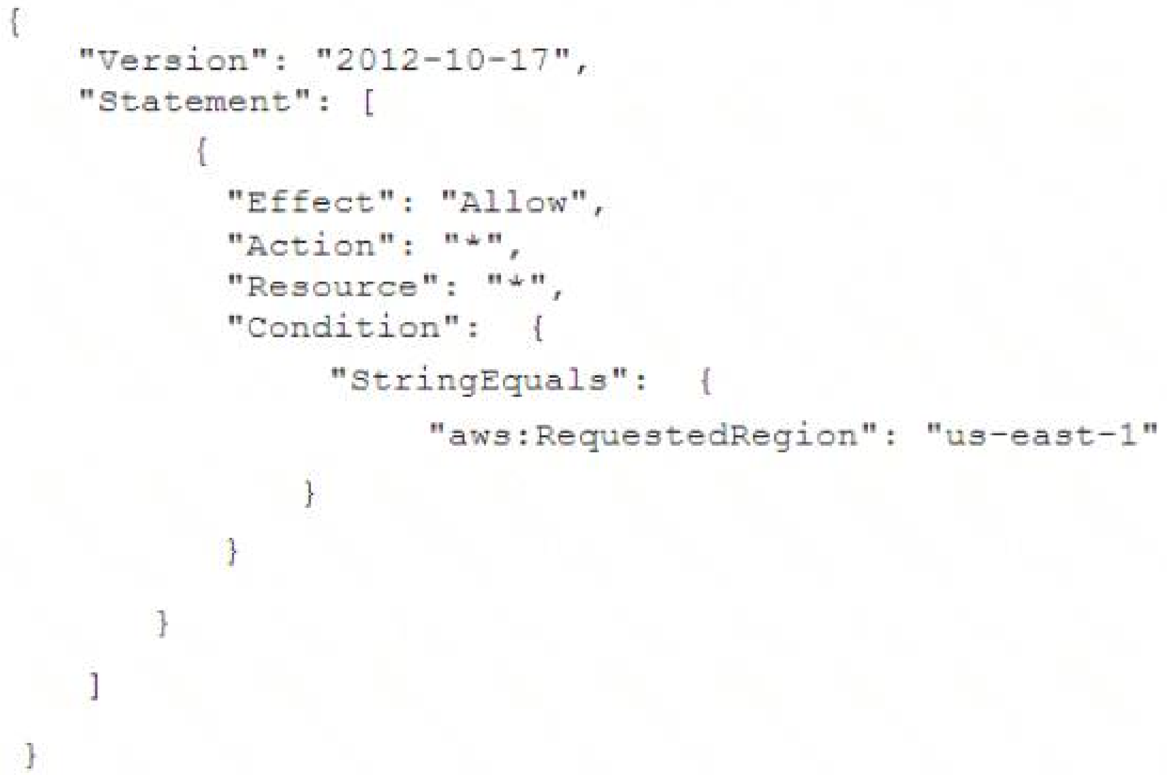
```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:DescribeKey",
  "kms:GenerateDataKey*",
  "kms:Encrypt",
  "kms:ReEncrypt*",
  "kms:Disable*",
  "kms:Decrypt"
 ],
```

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

Answer: B

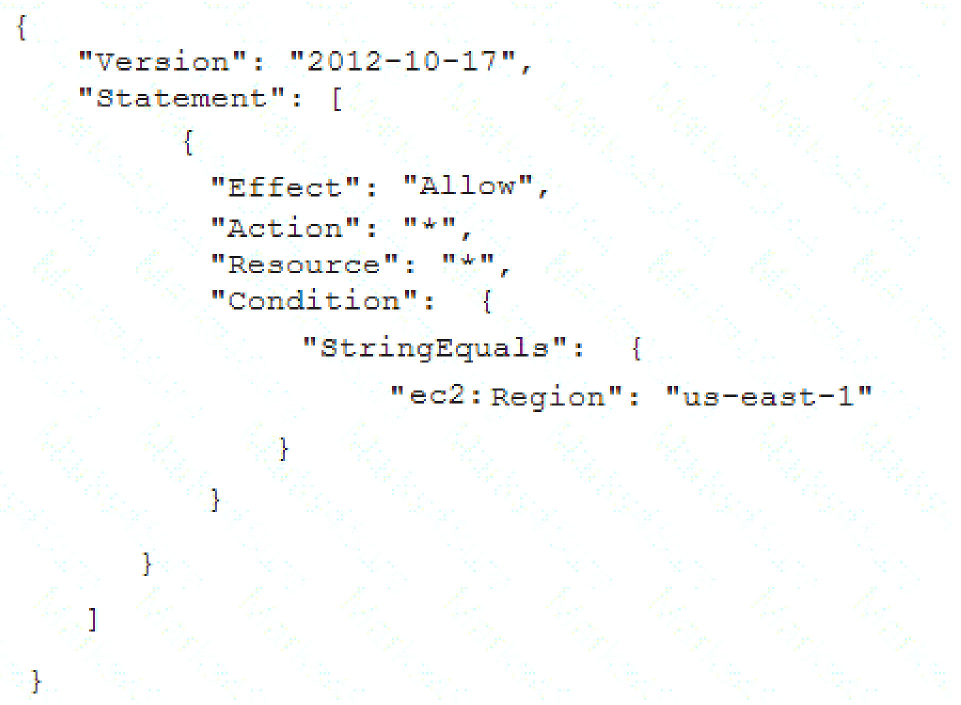
NEW QUESTION 13
- (Exam Topic 1)
To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.
What policy should the Engineer implement?

A



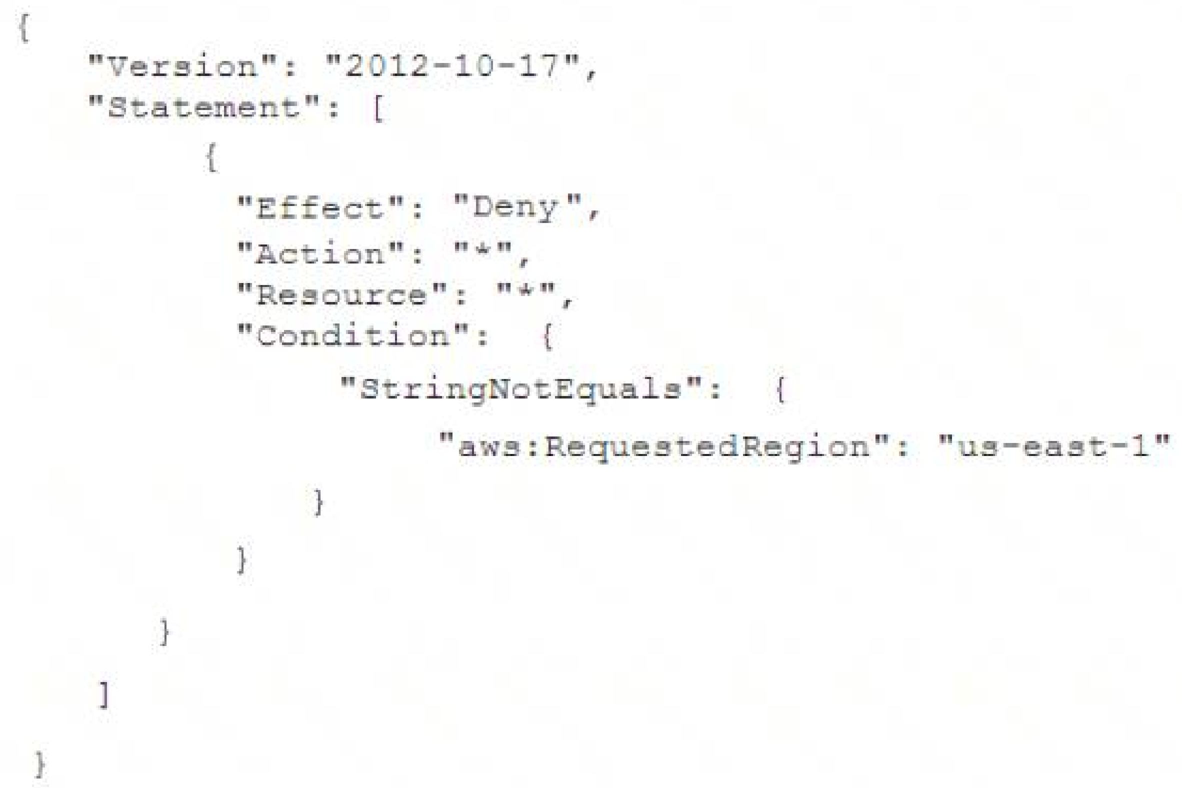
```
{
    "Version": "2012-10-17",
    "Statement": [
          {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*",
            "Condition":  {
                 "StringEquals":  {
                      "aws:RequestedRegion":  "us-east-1"
                 }
      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

B



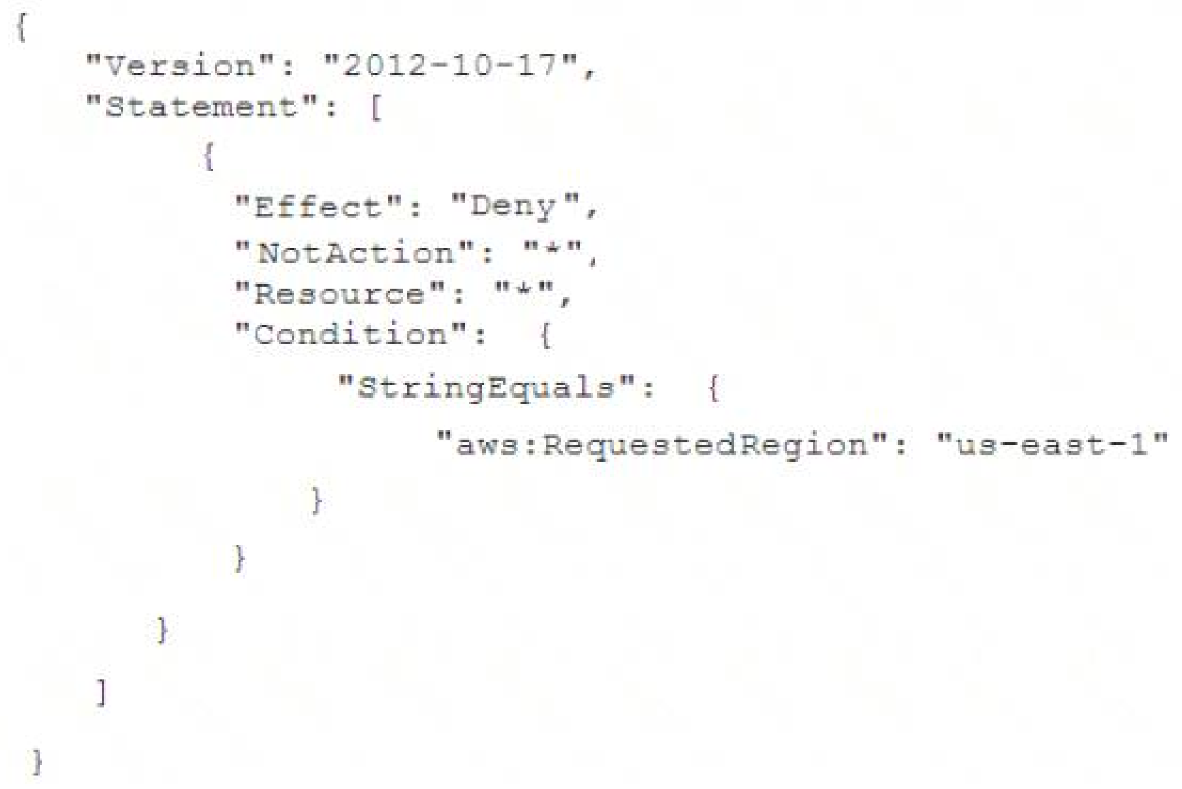
```
{
   "Version": "2012-10-17",
   "Statement": [
         {
          "Effect": "Allow",
          "Action": "*",
          "Resource": "*",
          "Condition":  {
               "StringEquals":  {
                    "ec2:Region": "us-east-1"
               }
          }
         }
     ]
}
```

C



```
{
   "Version": "2012-10-17",
   "Statement": [
         {
          "Effect": "Deny",
          "Action": "*",
          "Resource": "*",
          "Condition":  {
               "StringNotEquals":  {
                    "aws:RequestedRegion": "us-east-1"
               }
          }
         }
     ]
}
```

D



```
{
   "Version": "2012-10-17",
   "Statement": [
         {
          "Effect": "Deny",
          "NotAction": "*",
          "Resource": "*",
          "Condition":  {
               "StringEquals":  {
                    "aws:RequestedRegion": "us-east-1"
               }
          }
         }
     ]
}
```

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

Answer: A

NEW QUESTION 14
- (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 AWS PrivateLink to the VPC Then update the custom route table with a new route to AWS 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 the gateway

Answer: D

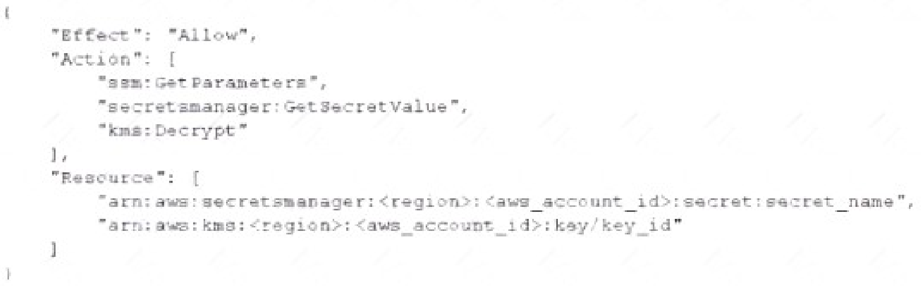
NEW QUESTION 19
- (Exam Topic 1)
A company uses SAML federation with AWS Identity and Access Management (IAM) to provide internal users with SSO for their AWS accounts. The company's identity provider certificate was rotated as part of its normal lifecycle. Shortly after, users started receiving the following error when attempting to log in:
"Error: Response Signature Invalid (Service: AWSSecuntyTokenService; Status Code: 400; Error Code: InvalidldentltyToken)"
A security engineer needs to address the immediate issue and ensure that it will not occur again. Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

A. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
B. Upload the new metadata file to the new IAM identity provider entity.
C. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
D. Generate a new metadata file and upload it to the IAM identity provider entit
E. Perform automated or manual rotation of the certificate when required.
F. Download a new copy of the SAML metadata file from the identity provider Upload the new metadata to the IAM identity provider entity configured for the SAML integration in question.
G. During the next certificate rotation period and before the current certificate expires, add a new certificate as the secondary to the identity provide
H. Generate a new copy of the metadata file and create a new IAM identity provider entit
I. Upload the metadata file to the new IAM identity provider entit
J. Performautomated or manual rotation of the certificate when required.
K. Download a new copy of the SAML metadata file from the identity provider Create a new IAM identity provider entit
L. Upload the new metadata file to the new IAM identity provider entit
M. Update the identity provider configurations to pass a new IAM identity provider entity name in the SAML assertion.

Answer: AD

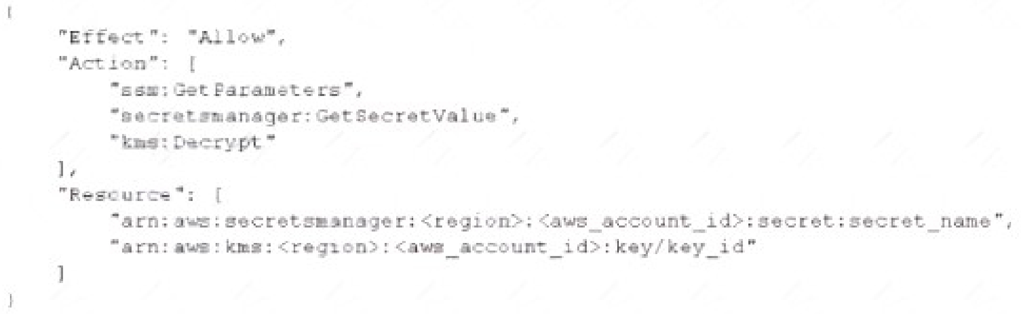
NEW QUESTION 24
- (Exam Topic 1)
A recent security audit identified that a company's application team injects database credentials into the environment variables of an AWS Fargate task. The company's security policy mandates that all sensitive data be encrypted at rest and in transit.
When combination 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 AWS Secrets Manager secret and specify the key/value pairs to be stored in this secret
C. Modify the application to pull credentials from the AWS 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 AWS Fargate instance, create a script to read the secret value from AWS Secret Manager, and inject the environment variable
G. Ask the application team to redeploy the application.

Answer: BEF

NEW QUESTION 27
- (Exam Topic 1)
A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all

use AWS. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary
What solution should the Engineer use to implement the appropriate access restrictions for the application?

A. Create a NACL to allow access on TCP port 443 from the 1;500 subsidiary CIDR block ranges.Associate the NACL to both the NLB and EC2 instances
B. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
C. Associate the security group to the NL
D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
E. Create an AWS PrivateLink endpoint service in the parent company account attached to the NL
F. Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoin
G. Use AWS PrivateLink interface endpoints in the 1,500 subsidiary AWS accounts to connect to the data processing application.
H. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
I. Associate the security group with EC2 instances.

Answer: D

NEW QUESTION 32
- (Exam Topic 1)
A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.
The company's security engineer created an AWS Organizations trail in the master account, enabled
server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.
Which factors could cause this issue? (Select TWO.)

A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.
B. The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.
C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for crypto graphical operations.

Answer: AD

NEW QUESTION 35
- (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 39
- (Exam Topic 1)
A company's development team is designing an application using AWS Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company's security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application's AWS services. The solution must minimize management overhead.
How should the security team prevent privilege escalation for both teams?

A. Enable AWS CloudTrai
B. Create a Lambda function that monitors the event history for privilege escalation events and notifies the security team.
C. Create a managed IAM policy for the permissions require
D. Reference the IAM policy as a permissions boundary within the development team's IAM role.
E. Enable AWS Organizations Create an SCP that allows the IAM CreateUser action but that has a condition that prevents API calls other than those required by the development team
F. Create an IAM policy with a deny on the IAMCreateUser action and assign the policy to the development tea
G. Use a ticket system to allow the developers to request new IAM roles for their application
H. The IAM roles will then be created by the security team.

Answer: A

NEW QUESTION 41
- (Exam Topic 1)
A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs)
Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

A. Log on to each EC2 instance, check and export the different software versions installed, and verify this against a list of current CVEs.
B. Install the Amazon Inspector agent on all development instances Build a custom rule package, and configure Inspector to perform a scan using this custom rule on all instances tagged as being in the development environment.
C. Install the Amazon Inspector agent on all development instances Configure Inspector to perform a scan using the CVE rule package on all instances tagged as being in the development environment.
D. Install the Amazon EC2 System Manager agent on all development instances Issue the Run command to EC2 System Manager to update all instances
E. Use AWS Trusted Advisor to check that all EC2 instances have been patched to the most recent versionof operating system and installed software.

Answer: CD

NEW QUESTION 45
- (Exam Topic 1)
A security engineer need to ensure their company’s uses of AWS meets AWS security best practices. As part of this, the AWS account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used. Which solution meets these requirements?

A. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification.
B. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification logs from S3 and generate notifications using Amazon SNS.
C. Set up a rule in AWS config to trigger root user event
D. Trigger an AWS Lambda function and generate notifications using Amazon SNS.
E. Use Amazon Inspector to monitor the usage of the root user and generate notifications using Amazon SNS

Answer: A

NEW QUESTION 48
- (Exam Topic 1)
A company uses multiple AWS accounts managed with AWS 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 AWS 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 AWS 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 AWS Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation
D. Use AWS 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 52
- (Exam Topic 1)
A company has multiple AWS accounts that are part of AW5 Organizations. The company's Security team wants to ensure that even those Administrators with full access to the company's AWS accounts are unable to access the company's Amazon S3 buckets
How should this be accomplished?

A. UseSCPs
B. Add a permissions boundary to deny access to Amazon S3 and attach it to all roles
C. Use an S3 bucket policy
D. Create a VPC endpoint for Amazon S3 and deny statements for access to Amazon S3

Answer: A

NEW QUESTION 55
- (Exam Topic 1)
A company has a serverless application for internal users deployed on AWS. The application uses AWS Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC The company uses AWS Systems Manager Parameter Store for storing database credentials.
A recent security review highlighted the following issues

> The Lambda function has internet access.
> The relational database is publicly accessible.
> The database credentials are not stored in an encrypted state.

Which combination of steps should the company take to resolve these security issues? (Select THREE)

A. Disable public access to the RDS database inside the VPC
B. Move all the Lambda functions inside the VPC.
C. Edit the IAM role used by Lambda to restrict internet access.
D. Create a VPC endpoint for Systems Manage
E. Store the credentials as a string paramete
F. Change the parameter type to an advanced parameter.
G. Edit the IAM role used by RDS to restrict internet access.
H. Create a VPC endpoint for Systems Manage
I. Store the credentials as a SecureString parameter.

Answer: ABE

NEW QUESTION 57
- (Exam Topic 1)
A company Is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The security team has the following requirements for the architecture:
• Data must be encrypted in transit.
• Data must be encrypted at rest.
• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Select THREE.)

A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket
B. Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
C. Add a bucket policy that includes a deny if a PutObject request does not include awsiSecureTcanspoct.
D. Add a bucket policy with ws: Sourcelpto Allow uploads and downloads from the corporate intranet only.
E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-sairv9r-side-enctyption: "aws: kms".
F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: BDF

NEW QUESTION 60
- (Exam Topic 1)
While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
What action should be performed to allow the ping to work?

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

Answer: D

NEW QUESTION 64
- (Exam Topic 1)
A security engineer is responsible for providing secure access to AWS resources for thousands of developer in a company’s corporate identity provider (idp). The developers access a set of AWS services from the corporate premises using IAM credential. Due to the velum of require for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid provisioning delays. The causes concern about overall security for the security engineer.
Which actions will meet the program requirements that address security?

A. Create an Amazon CloudWatch alarm for AWS CloudTrail Events Create a metric filter to send a notification when me same set of IAM credentials is used by multiple developer
B. Create a federation between AWS and the existing corporate IdP Leverage IAM roles to provide federated access to AWS resources
C. Create a VPN tunnel between the corporate premises and the VPC Allow permissions to all AWS services only if it originates from corporate premises.
D. Create multiple IAM rotes for each IAM user Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
A city is implementing an election results reporting website that will use Amazon GoudFront The website runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. Election results are updated hourly and are stored as .pdf tiles in an Amazon S3 bucket. A Security Engineer needs to ensure that all external access to the website goes through CloudFront.
Which solution meets these requirements?

A. Create an IAM role that allows CloudFront to access the specific S3 bucke
B. Modify the S3 bucket policy to allow only the new IAM role to access its content
C. Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
D. Create an IAM role that allows CloudFront to access the specific S3 bucke
E. Modify the S3 bucket policy to allow only the new IAM role to access its content
F. Associate the ALB with a security group that allows only incoming traffic from the CloudFront service to communicate with the ALB.
G. Create an origin access identity (OAI) in CloudFron
H. Modify the S3 bucket policy to allow only the new OAI to access the bucket content
I. Create an interface VPC endpoint for CloudFront to securely communicate with the ALB.
J. Create an origin access identity (OAI) in CloudFron
K. Modify the S3 bucket policy to allow only the new OAI to access the bucket content
L. Associate the ALB with a security group that allows onlyincoming traffic from the CloudFront service to communicate with the ALB.

Answer: C

NEW QUESTION 71
- (Exam Topic 1)
A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.
Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data
Which solution will meet these requirements?

A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data
B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to generate and store a data encryption key for each customer.
C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys
D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store Use CloudHSM to generate and store a new CMK for each customer.

Answer: A

NEW QUESTION 75
- (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 AWS 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.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html You can disable the service for existing (running or stopped) ec2 instances. https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html

NEW QUESTION 80
- (Exam Topic 1)
A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?

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

Answer: B

NEW QUESTION 85
- (Exam Topic 1)
A company recently performed an annual security assessment of its AWS 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 AWS 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 AWS Artifact to archive AWS CloudTrail logs Configure AWS 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 AWS CloudTrail to provide a notification when a policy change is made to resources.
E. Create an AWS CloudTrail trail that stores audit logs in Amazon S3. Configure an AWS Config rule to provide a notif cation when a policy change is made to resources.

Answer: A

NEW QUESTION 90
- (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 94
- (Exam Topic 1)
A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:
• HTTPS needs to be enforced for all data in transit with specific ciphers.
• The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

A. Set up an S3 bucket policy with the awssecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher

B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with AWS WAF to allow access from the CloudFront IP ranges.
C. Set up an S3 bucket policy with the aws:securetransport ke
D. Configure the CloudFront origin access identity (OAI) with the S3 bucke
E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
F. Modify the CloudFront distribution to use AWS WA
G. Force HTTPS on the S3 bucket with specific ciphers in the bucket polic
H. Configure an HTTPS listener only for the AL
I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
J. Modify the CloudFront distribution to use the ALB as the origi
K. Enforce an HTTPS listener on the AL
L. Create a path-based routing rule on the ALB with proxies that connect lo Amazon S3. Create a bucket policy to allow access from these proxies only.A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with AWS Systems Manager Session Manage
M. A security engineer has installed the Systems Manager Agent on all server
N. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to the
O. The security engineer needs to perform verification steps before Session Manager will work on the servers.Which combination of steps should the security engineer perform? (Select THREE.)
P. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.
Q. Enable the advanced-instances tier in Systems Manager.
R. Create a managed-instance activation for the on-premises servers.
S. Reconfigure the Systems Manager Agent with the activation code and ID.
T. Assign an IAM role to all of the on-premises servers.
. Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 95
- (Exam Topic 1)
A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes The software engineering team needs to make changes that will address the audit findings.
Which set of steps should the software engineering team take?

A. Use an AWS Key Management Service (AWS KMS) CM
B. Encrypt the data at rest.
C. Use AWS Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.
D. Use a DynamoDB encryption clien
E. Use client-side encryption and sign the table items
F. Use the AWS Encryption SD
G. Use client-side encryption and sign the table items.

Answer: A

NEW QUESTION 96
- (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 AWS 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

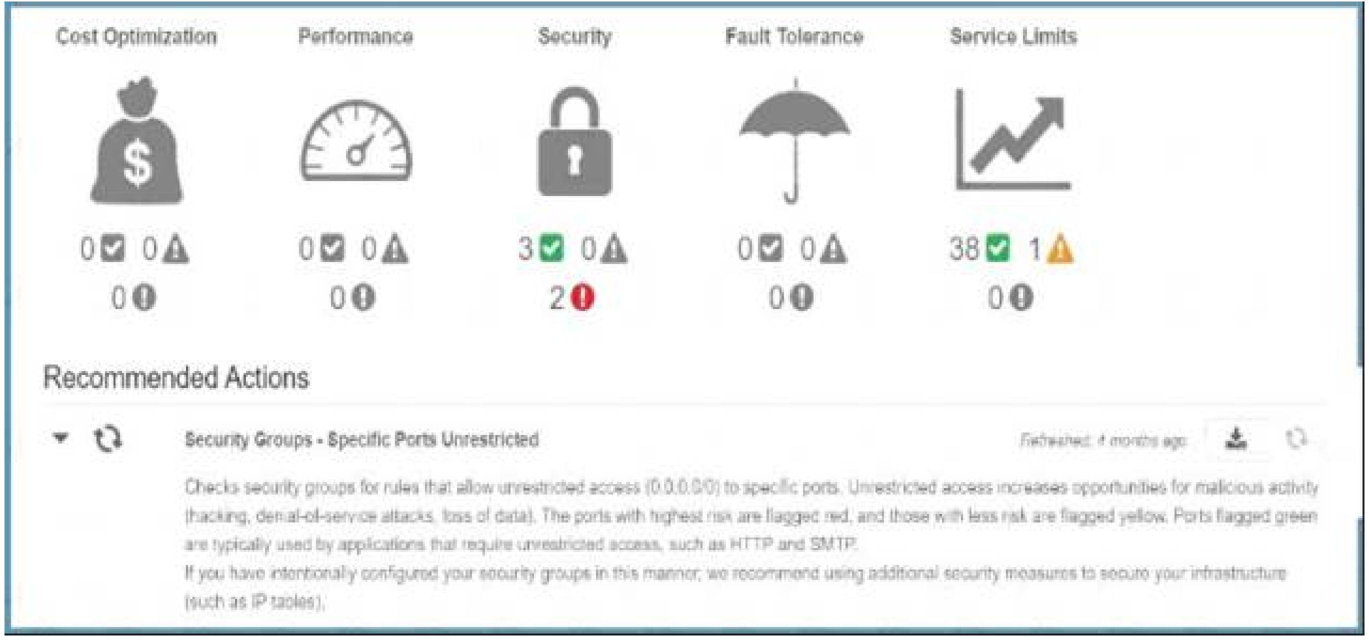
NEW QUESTION 101
- (Exam Topic 2)
Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?
Please select:

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

Answer: B

Explanation:
The AWS 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 AWS Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg



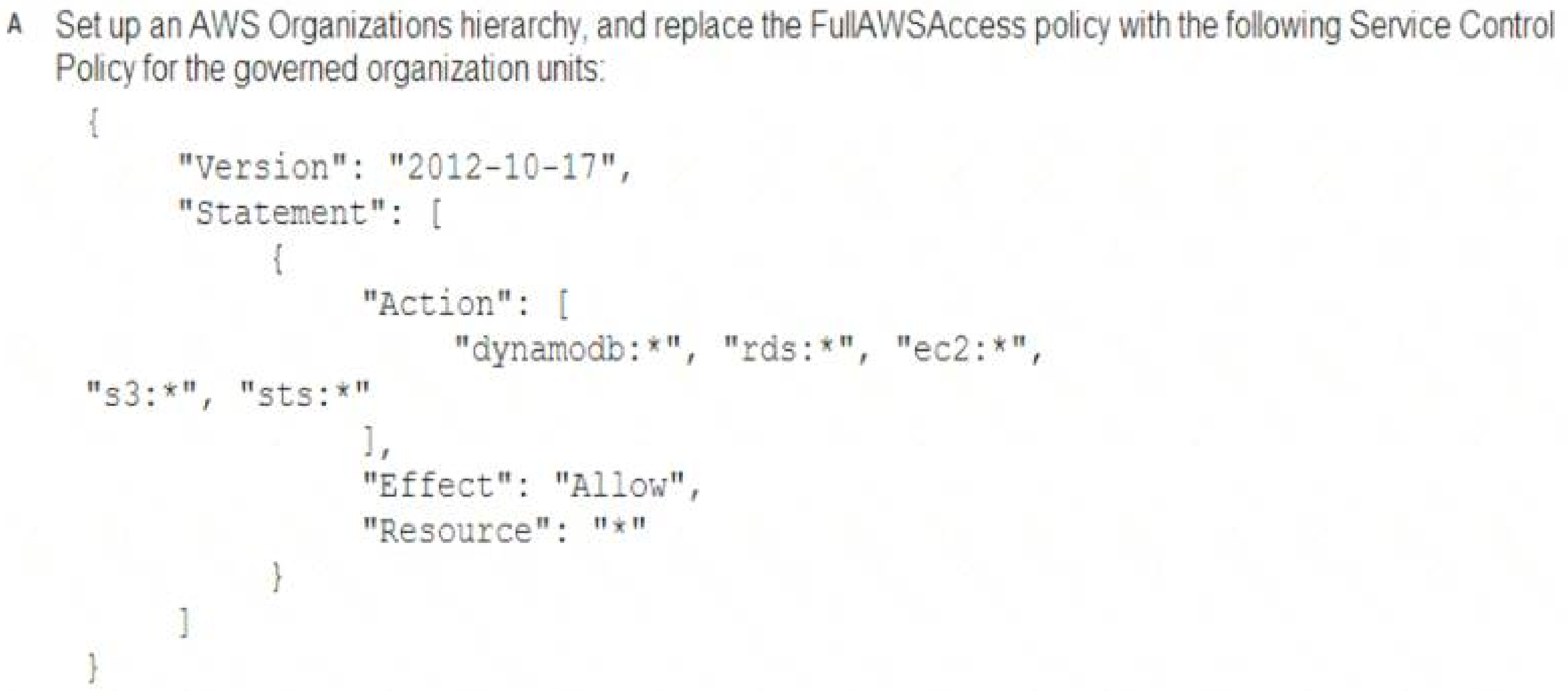
Recommended Actions

Security Groups - Specific Ports Unrestricted

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). The ports with highest risk are flagged red, and those with less risk are flagged yellow. Ports flagged green are typically used by applications that require unrestricted access, such as HTTP and SMTP.
If you have intentionally configured your security groups in this manner, we recommend using additional security measures to secure your infrastructure (such as IP tables).

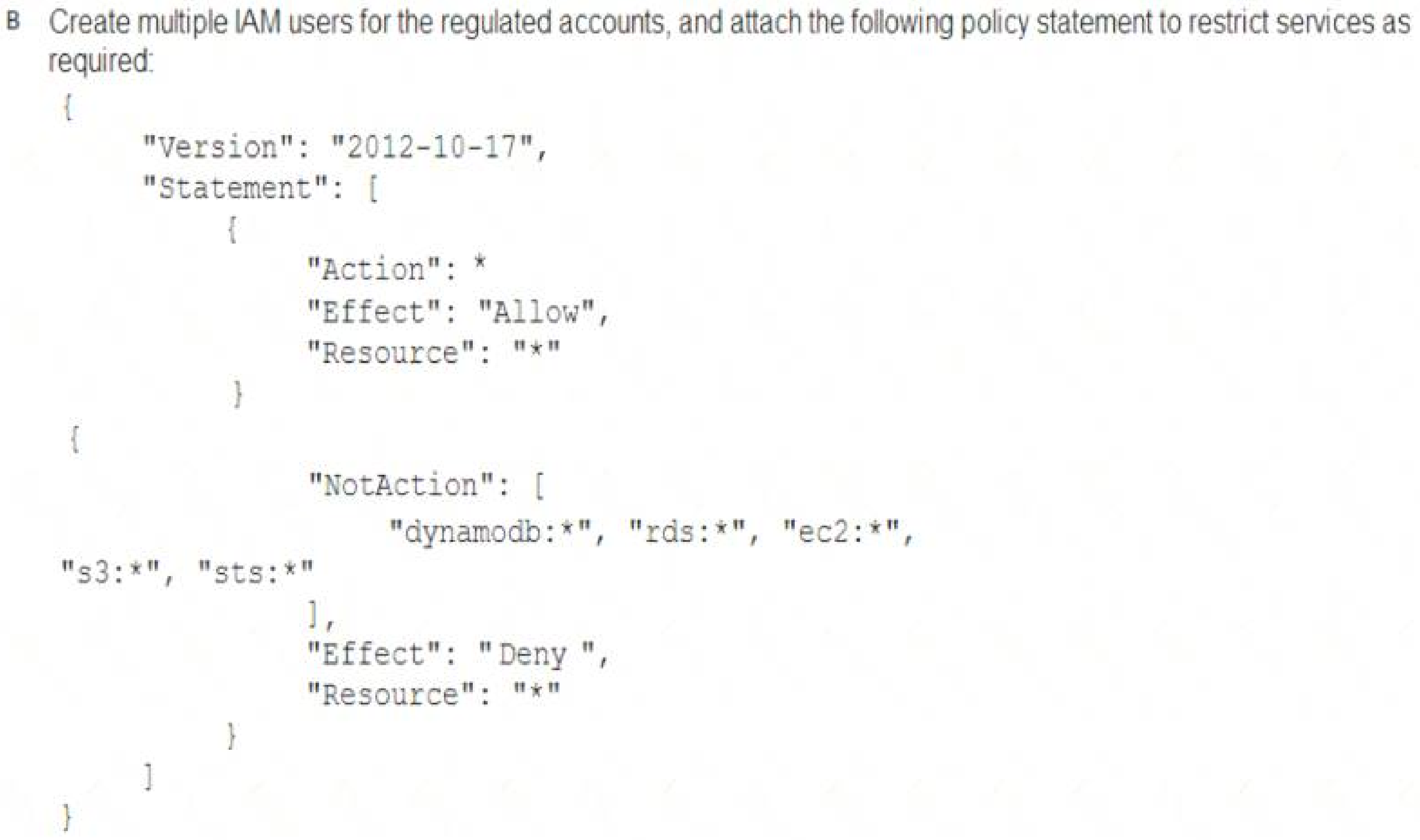
Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.
Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.
Option Dis partially valid but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

NEW QUESTION 106
- (Exam Topic 2)
A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and AWS STS in specific accounts.
What is a scalable and efficient approach to meet this requirement?



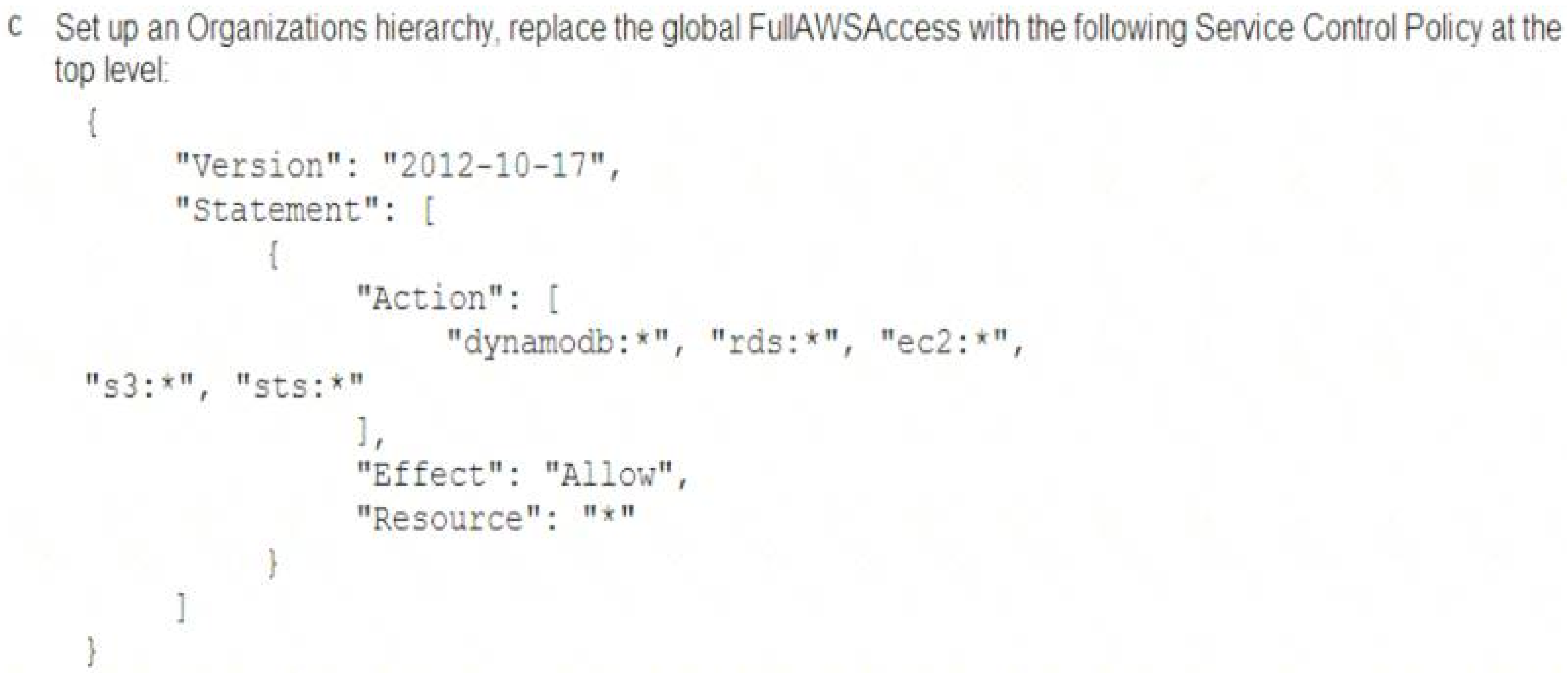
A Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Allow",
               "Resource": "*"
          }
     ]
}
```



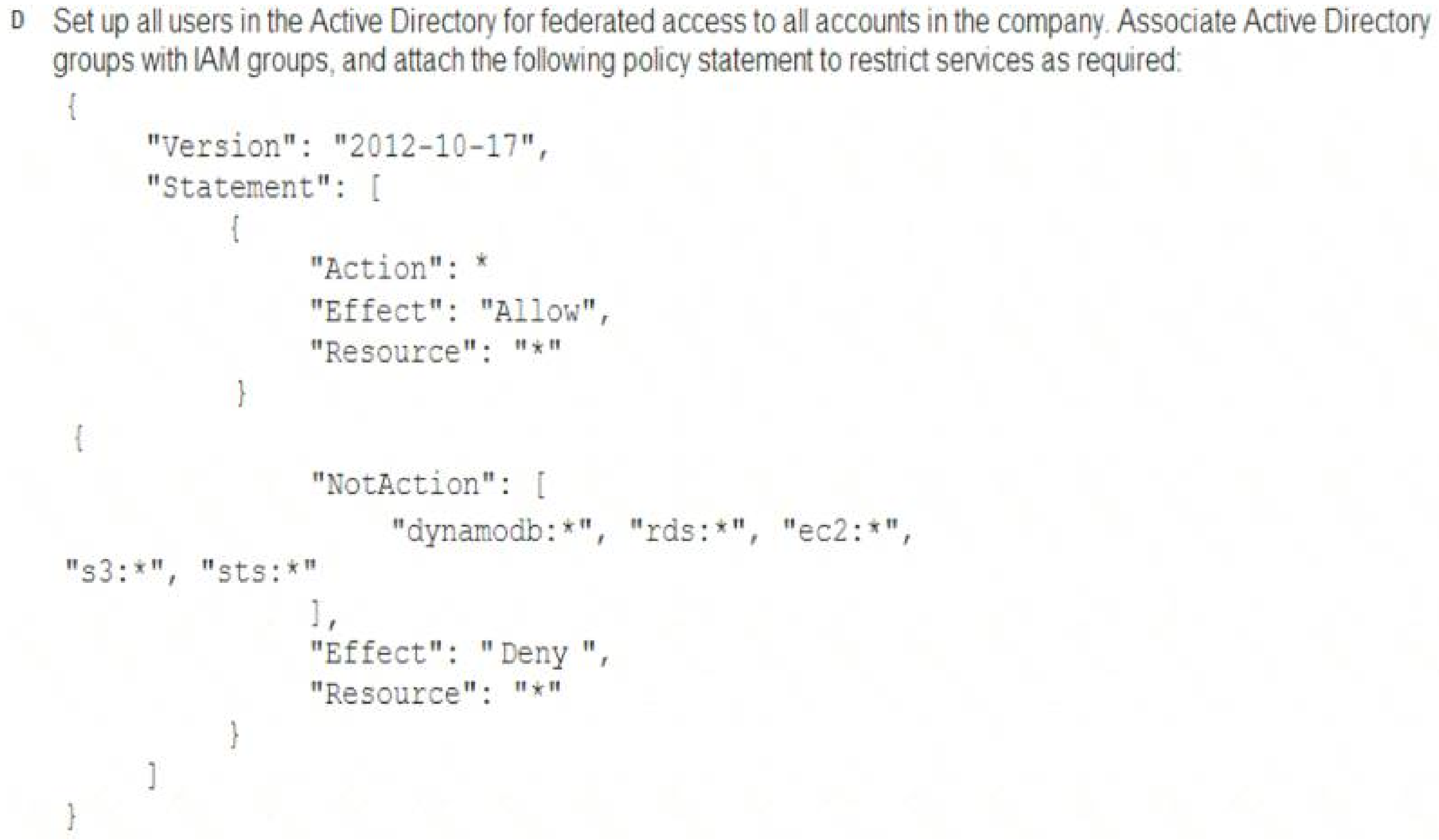
B Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": *
               "Effect": "Allow",
               "Resource": "*"
          }
{
               "NotAction": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Deny ",
               "Resource": "*"
          }
     ]
}
```



C Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
 {
      "Version": "2012-10-17",
      "Statement": [
           {
                "Action": [
                     "dynamodb:*", "rds:*", "ec2:*",
 "s3:*", "sts:*"
                ],
                "Effect": "Allow",
                "Resource": "*"
           }
      ]
 }
```



D Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required:

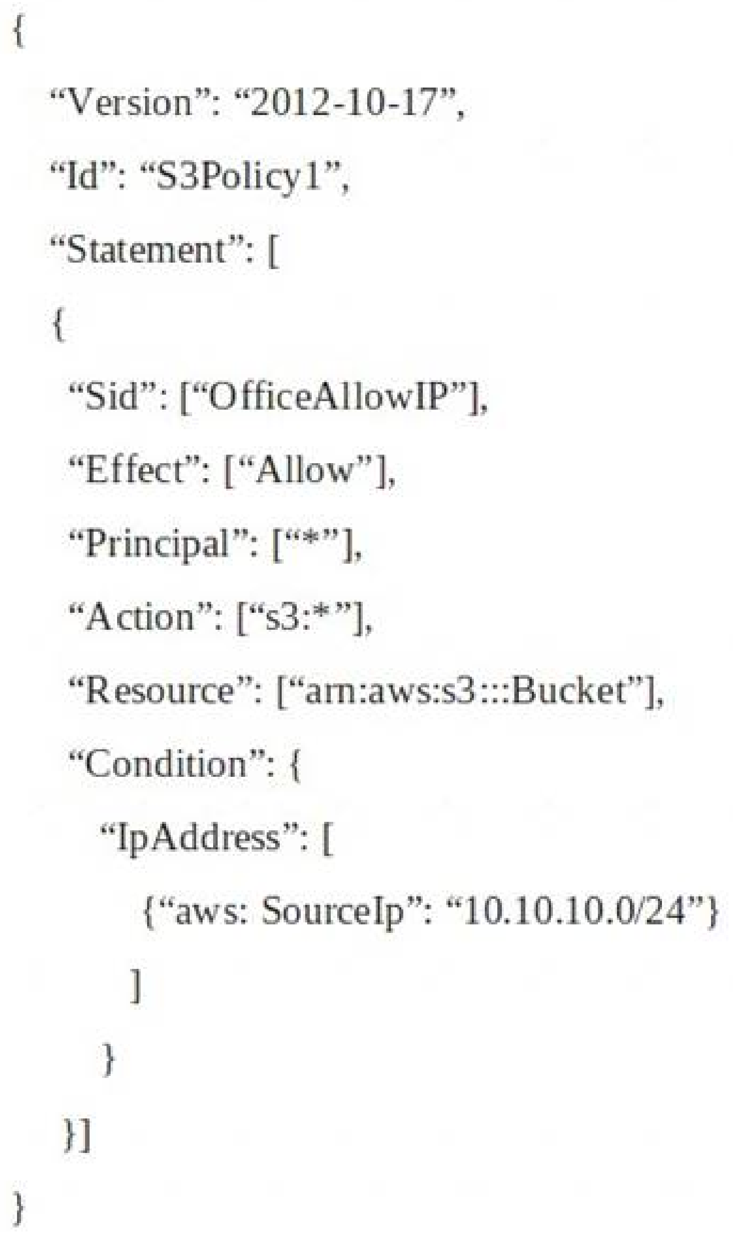
```
 {
      "Version": "2012-10-17",
      "Statement": [
           {
                "Action": *
                "Effect": "Allow",
                "Resource": "*"
           }
 {
                "NotAction": [
                     "dynamodb:*", "rds:*", "ec2:*",
 "s3:*", "sts:*"
                ],
                "Effect": " Deny ",
                "Resource": "*"
           }
      ]
 }
```

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

Answer: A

Explanation:
It says specific accounts which mean specific governed OUs under your organization and you apply specific service control policy to these OUs.

NEW QUESTION 109
- (Exam Topic 2)
A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized AWS IAM user from the IP address range 10.10.10.0/24:



```
{
   “Version”: “2012-10-17”,
   “Id”: “S3Policy1”,
   “Statement”: [
   {
    “Sid”: [“OfficeAllowIP”],
    “Effect”: [“Allow”],
    “Principal”: [“*”],
    “Action”: [“s3:*”],
    “Resource”: [“arn:aws:s3:::Bucket”],
    “Condition”: {
      “IpAddress”: [
         {“aws: SourceIp”: “10.10.10.0/24”}
        ]
      }
    }]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.
What does the Administrator need to change to grant access to the user?

A. Change the “Resource” from “arn: aws:s3:::Bucket” to “arn:aws:s3:::Bucket/*”.
B. Change the “Principal” from “*” to {AWS:”arn:aws:iam: : account-number: user/username”}
C. Change the “Version” from “2012-10-17” to the last revised date of the policy
D. Change the “Action” from [“s3:*”] to [“s3:GetObject”, “s3:ListBucket”]

Answer: A

NEW QUESTION 113
- (Exam Topic 2)
An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, AWS Lambda functions must issue queries to the RDS database by using the same database credentials.
The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.
What should the Security Engineer do to meet these requirements?

A. Store the database credentials in AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS KMS by using the EC2 and Lambda service principals in the role’s trust polic
B. Add the role to an EC2 instance profil
C. Attach the instance profile to the EC2 instance
D. Set up Lambda to use the new role for execution.
E. Store the database credentials in AWS KM
F. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role’s trust polic
G. Add the role to an EC2 instance profil
H. Attach the instance profile to the EC2 instances and the Lambda function.
I. Store the database credentials in AWS Secrets Manage
J. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role’s trust polic
K. Add the role to an EC2 instance profil
L. Attach the instance profile to the EC2 instances and the Lambda function.
M. Store the database credentials in AWS Secrets Manage
N. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role’s trust polic
O. Add the role to an EC2 instance profil
P. Attach the instance profile to the EC2 instance
Q. Set up Lambda to use the new role for execution.

Answer: D

NEW QUESTION 117
- (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 AWS Config to review the IAM policy assigned to users before and after the incident.
B. Run the GenerateCredentialReport via the AWS CLI, and copy the output to Amazon S3 daily for auditing purposes.
C. Copy AWS CloudFormation templates to S3, and audit for changes from the template.
D. Use Amazon EC2 Systems Manager to deploy images, and review AWS CloudTrail logs for changes.

Answer: A

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

NEW QUESTION 122
- (Exam Topic 2)
A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.
Which application flow would meet the data protection requirements on AWS?

A. Digitized files -> Amazon Kinesis Data Analytics
B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Answer: B

NEW QUESTION 123
- (Exam Topic 2)
A Security Engineer received an AWS Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.
Which action should the Engineer take based on this situation? (Choose three.)

A. Use AWS Artifact to capture an exact image of the state of each instance.
B. Create EBS Snapshots of each of the volumes attached to the compromised instances.
C. Capture a memory dump.
D. Log in to each instance with administrative credentials to restart the instance.
E. Revoke all network ingress and egress except for to/from a forensics workstation.
F. Run Auto Recovery for Amazon EC2.

Answer: BEF

NEW QUESTION 127
- (Exam Topic 2)
A company has Windows Amazon EC2 instances in a VPC that are joined to on-premises Active Directory servers for domain services. The security team has enabled Amazon GuardDuty on the AWS account to alert on issues with the instances.
During a weekly audit of network traffic, the Security Engineer notices that one of the EC2 instances is attempting to communicate with a known command-and-control server but failing. This alert does not show up in GuardDuty.
Why did GuardDuty fail to alert to this behavior?

A. GuardDuty did not have the appropriate alerts activated.
B. GuardDuty does not see these DNS requests.
C. GuardDuty only monitors active network traffic flow for command-and-control activity.
D. GuardDuty does not report on command-and-control activity.

Answer: B

Explanation:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_backdoor.html

NEW QUESTION 130
- (Exam Topic 2)
Your company is planning on hosting an internal network in AWS. 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 AWS Certificate Manager
C. Consider using AWS Access keys to generate the certificates
D. Consider using AWS Trusted Advisor for managing the certificates

Answer: B

Explanation:
The AWS Documentation mentions the following
ACM is tightly linked with AWS 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", AWS 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.aws.amazon.com/acm/latest/userguide/acm-overview.html

The correct answer is: Consider using AWS Certificate Manager Submit your Feedback/Queries to our Experts

NEW QUESTION 134
- (Exam Topic 2)
A Security Engineer is trying to determine whether the encryption keys used in an AWS service are in compliance with certain regulatory standards.
Which of the following actions should the Engineer perform to get further guidance?

A. Read the AWS Customer Agreement.
B. Use AWS Artifact to access AWS compliance reports.
C. Post the question on the AWS Discussion Forums.
D. Run AWS Config and evaluate the configuration outputs.

Answer: A

Explanation:
https://aws.amazon.com/artifact/

NEW QUESTION 138
- (Exam Topic 2)
A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.
Which approach will meet these requirements while protecting the external certificate during a breach?

A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.
B. Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instance
C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
D. Generate an internal self-signed certificate and apply it to the instance
E. Use AWS Certificate Manager to generate a new external certificate for the EL
F. Have the ELB decrypt traffic, and route andre-encrypt with the internal certificate.
G. Upload a new external certificate to the load balance
H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C

NEW QUESTION 142
- (Exam Topic 2)
The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.
What is causing this situation?

A. Application Load Balancers do not support older web browsers.
B. The Perfect Forward Secrecy settings are not configured correctly.
C. The intermediate certificate is installed within the Application Load Balancer.
D. The cipher suites on the Application Load Balancers are blocking connections.

Answer: D

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

NEW QUESTION 143
- (Exam Topic 2)
An application makes calls to AWS services using the AWS 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 146
- (Exam Topic 2)
A company is using CloudTrail to log all AWS API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.
What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below
Please select:

A. Create an S3 bucket in a dedicated log account and grant the other accounts write only acces
B. Deliver all log files from every account to this S3 bucket.
C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
D. Run the function every 10 minutes.
E. Enable CloudTrail log file integrity validation

F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
G. Create a Security Group that blocks all traffic except calls from the CloudTrail servic
H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:
The AWS Documentation mentions the following
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log fill integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.
Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-loe-file-validation-intro.htmll For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.htm
The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation
Submit your Feedback/Queries to our Experts

NEW QUESTION 151
- (Exam Topic 2)
What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Choose two.)

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

Answer: CE

NEW QUESTION 154
- (Exam Topic 2)
You have a vendor that needs access to an AWS resource. You create an AWS user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?
Please select:

A. An AWS Managed Policy
B. An Inline Policy
C. A Bucket Policy
D. A bucket ACL

Answer: B

Explanation:
The AWS Documentation gives an example on such a case
Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that if s applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Management Console to delete that principal entit the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.
Option A is invalid because AWS Managed Polices are ok for a group of users, but for individual users, inline policies are better.
Option C and D are invalid because they are specifically meant for access to S3 buckets For more information on policies, please visit the following URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access managed-vs-inline
The correct answer is: An Inline Policy Submit your Feedback/Queries to our Experts

NEW QUESTION 158
- (Exam Topic 2)
While analyzing a company's security solution, a Security Engineer wants to secure the AWS account root user.
What should the Security Engineer do to provide the highest level of security for the account?

A. Create a new IAM user that has administrator permissions in the AWS accoun
B. Delete the password forthe AWS account root user.
C. Create a new IAM user that has administrator permissions in the AWS accoun
D. Modify the permissions for the existing IAM users.
E. Replace the access key for the AWS account root use
F. Delete the password for the AWS account root user.
G. Create a new IAM user that has administrator permissions in the AWS accoun
H. Enable multi-factor authentication for the AWS account root user.

Answer: D

Explanation:
If you continue to use the root user credentials, we recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

NEW QUESTION 161
- (Exam Topic 2)
The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault.
What is the MOST cost-effective way to correct this?

A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
C. Update the policy, keeping the vault lock in place.
D. Update the policy and call initiate-vault-lock again to apply the new policy.

Answer: A

Explanation:
Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires. Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API. https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html

NEW QUESTION 166
- (Exam Topic 2)
An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.
What techniques will limit lateral movement and allow evidence gathering?

A. Remove the instance from the load balancer and terminate it.
B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
C. Reboot the instance and check for any Amazon CloudWatch alarms.
D. Stop the instance and make a snapshot of the root EBS volume.

Answer: B

Explanation:
https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

NEW QUESTION 170
- (Exam Topic 2)
The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.
How can the InfoSec team ensure compliance with this mandate?

A. Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
B. Patch all running instances by using AWS Systems Manager.
C. Deploy AWS Config rules and check all running instances for compliance.
D. Define a metric filter in Amazon CloudWatch Logs to verify compliance.

Answer: C

Explanation:
https://docs.aws.amazon.com/config/latest/developerguide/approved-amis-by-id.html

NEW QUESTION 174
- (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 AWS Documentation mentions the following
AWS 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 AWS Patch Manager, please visit the below URL:
https://docs.aws.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 176
- (Exam Topic 2)
An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.
What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

A. Configure and assign an MFA device to the role used by the instances.
B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
C. Verify that the access key attached to the role used by the instances is active.
D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
E. Verify that the role attached to the instances contains policies that allow access to the queue.

Answer: BE

NEW QUESTION 178
- (Exam Topic 2)
A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS 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 AWS 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 AWS 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 AWS Organizations -Only service control policy (SCP) are supported https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

NEW QUESTION 182
- (Exam Topic 2)
A company plans to move most of its IT infrastructure to AWS. The company wants to leverage its existing on-premises Active Directory as an identity provider for AWS.
Which steps should be taken to authenticate to AWS 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 AWS 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://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-a

NEW QUESTION 187
- (Exam Topic 2)
Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

A. Turn on Cloud trail and carry out the penetration test
B. Turn on VPC Flow Logs and carry out the penetration test
C. Submit a request to AWS Support
D. Use a custom AWS Marketplace solution for conducting the penetration test

Answer: C

Explanation:
This concept is given in the AWS Documentation
How do I submit a penetration testing request for my AWS resources? Issue
I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?
Resolution
Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.
AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.
If your request is approved, you'll receive an authorization number.
Option A.B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests

For more information on penetration testing, please visit the below URL
* https://aws.amazon.com/security/penetration-testing/
* https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/ (
The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

NEW QUESTION 188
- (Exam Topic 2)
Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.
What steps are necessary to identify the cause of this phenomenon? (Choose two.)

A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
E. Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

Answer: AB

Explanation:
https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%

NEW QUESTION 190
- (Exam Topic 2)
An AWS Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.
Which of the following explains why the logs are not available?

A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
B. The Lambda function was executed by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
D. The version of the Lambda function that was executed was not current.

Answer: A

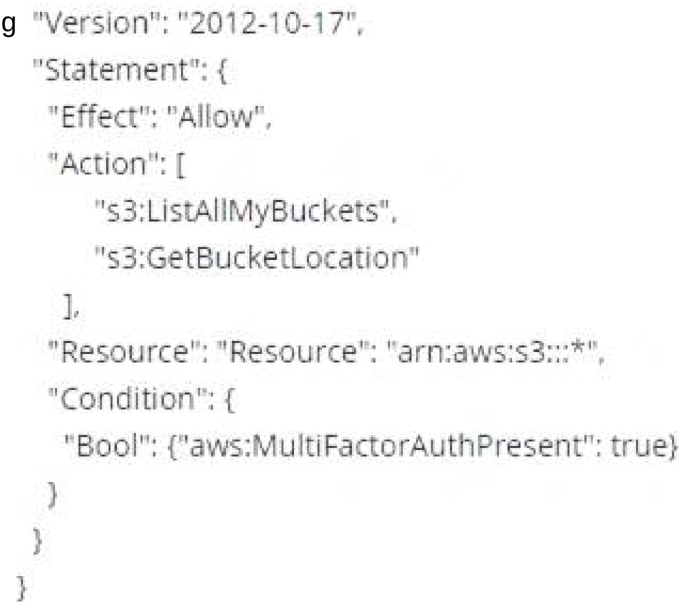
NEW QUESTION 193
- (Exam Topic 2)
During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects 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 AWS 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

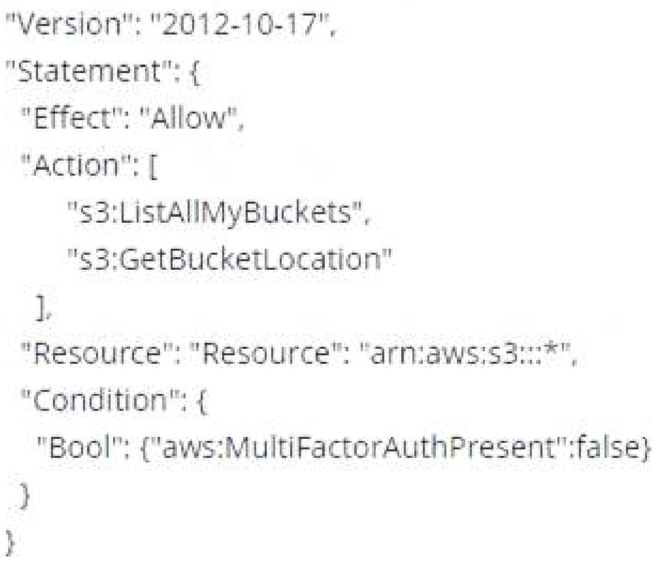
NEW QUESTION 198
- (Exam Topic 2)
You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

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



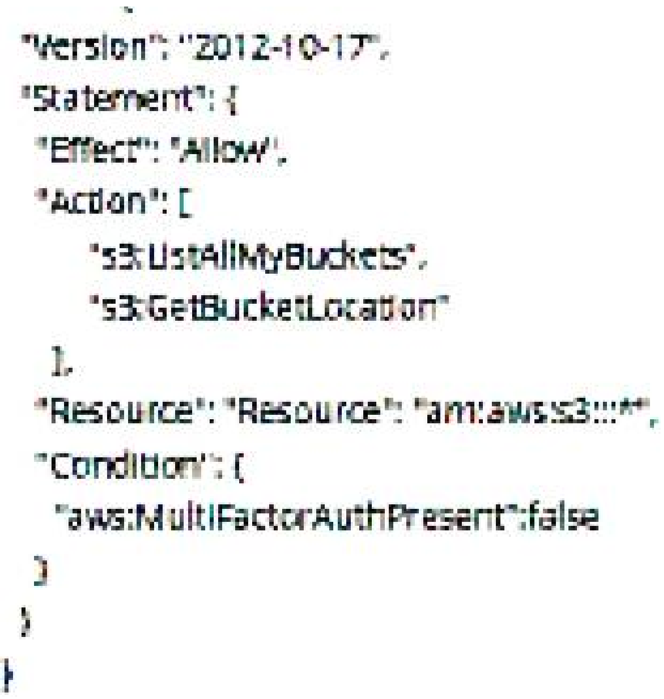
```
"Version": "2012-10-17",
"Statement": {
 "Effect": "Allow",
 "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
   ],
 "Resource": "Resource": "arn:aws:s3:::*",
 "Condition": {
   "Bool": {"aws:MultiFactorAuthPresent": true}
 }
}
}
```

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



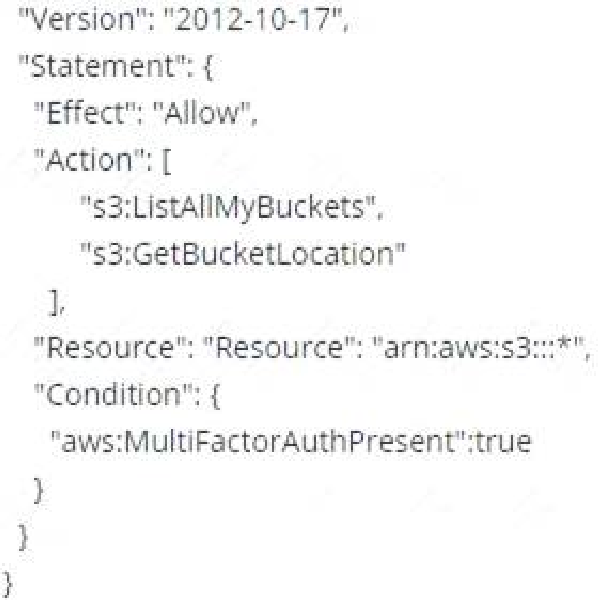
```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
    ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent":false}
  }
}
```

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



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

D. 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": {
    "aws:MultiFactorAuthPresent":true
  }
 }
}
```

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 aws: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 201
- (Exam Topic 2)
An organization has three applications running on AWS, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an AWS KMS Customer Master Key (CMK).
What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

A. Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.
B. Have each application assume an IAM role that provides permissions to use the AWS Certificate Manager CMK.
C. Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.
D. Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.

Answer: C

NEW QUESTION 202
- (Exam Topic 2)
A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.
Which solution meets these requirements?

A. Use AWS KMS with AWS managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.
B. Use KMS with AWS imported key material and then use the DeletelmportedKeyMaterial API to remove the key material if necessary.
C. Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.
D. Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.

Answer: C

Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-delete-key-material.html

NEW QUESTION 205
- (Exam Topic 2)
A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.
What should the Security Engineer use to accomplish this?

A. Server-side encryption with Amazon S3-managed keys (SSE-S3)
B. Server-side encryption with AWS KMS-managed keys (SSE-KMS)
C. Server-side encryption with customer-provided keys (SSE-C)
D. Client-side encryption with an AWS KMS-managed CMK

Answer: B

Explanation:
Reference https://aws.amazon.com/s3/faqs/

NEW QUESTION 209
- (Exam Topic 2)
Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.
B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Answer: B

Explanation:
"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key."
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

NEW QUESTION 212
- (Exam Topic 2)
The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.
Which architecture should the Security Engineer use to meet these requirements?

A. Use AWS Shield to scan inbound traffic for web exploit
B. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
C. Use AWS Shield to scan inbound traffic for web exploit
D. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.
E. Use AWS WAF to scan inbound traffic for web exploit
F. Use VPC Flow Logs and AWS Lambda torestrict egress traffic to specific whitelisted URLs.
G. Use AWS WAF to scan inbound traffic for web exploit
H. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.

Answer: D

Explanation:
AWS Shield is mainly for DDos Attacks.AWS WAF is mainly for some other types of attacks like Injection and XSS etcIn this scenario, It seems it is WAF functionality that is needed.VPC logs do show the source and destination IP and Port , they never show any URL .. because URL are level 7 while VPC are concerned about lover network levels.
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

NEW QUESTION 214
- (Exam Topic 2)
Which of the following are valid event sources that are associated with web access control lists that trigger AWS WAF rules? (Choose two.)

A. Amazon S3 static web hosting
B. Amazon CloudFront distribution
C. Application Load Balancer
D. Amazon Route 53
E. VPC Flow Logs

Answer: BC

Explanation:
A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon API Gateway API, Amazon CloudFront distribution or Application Load Balancer responds to.

NEW QUESTION 219
- (Exam Topic 2)
A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.
What would be the BEST way to reduce the potential impact of these attacks in the future?

A. Use custom route tables to prevent malicious traffic from routing to the instances.
B. Update security groups to deny traffic from the originating source IP addresses.
C. Use network ACLs.
D. Install intrusion prevention software (IPS) on each instance.

Answer: D

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html NACL has limit 20 (can increase to maximum 40 rule), and more rule will make more low-latency

NEW QUESTION 221
- (Exam Topic 2)
You have enabled Cloudtrail logs for your company's AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?
Please select:

A. Enable SSL certificates for the Cloudtrail logs
B. There is no need to do anything since the logs will already be encrypted
C. Enable Server side encryption for the trail
D. Enable Server side encryption for the destination S3 bucket

Answer: B

Explanation:
The AWS Documentation mentions the following.
By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.
Option A.C and D are not valid since logs will already be encrypted
For more information on how Cloudtrail works, please visit the following URL: https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/how-cloudtrail-works.htmll
The correct answer is: There is no need to do anything since the logs will already be encrypted Submit your Feedback/Queries to our Experts

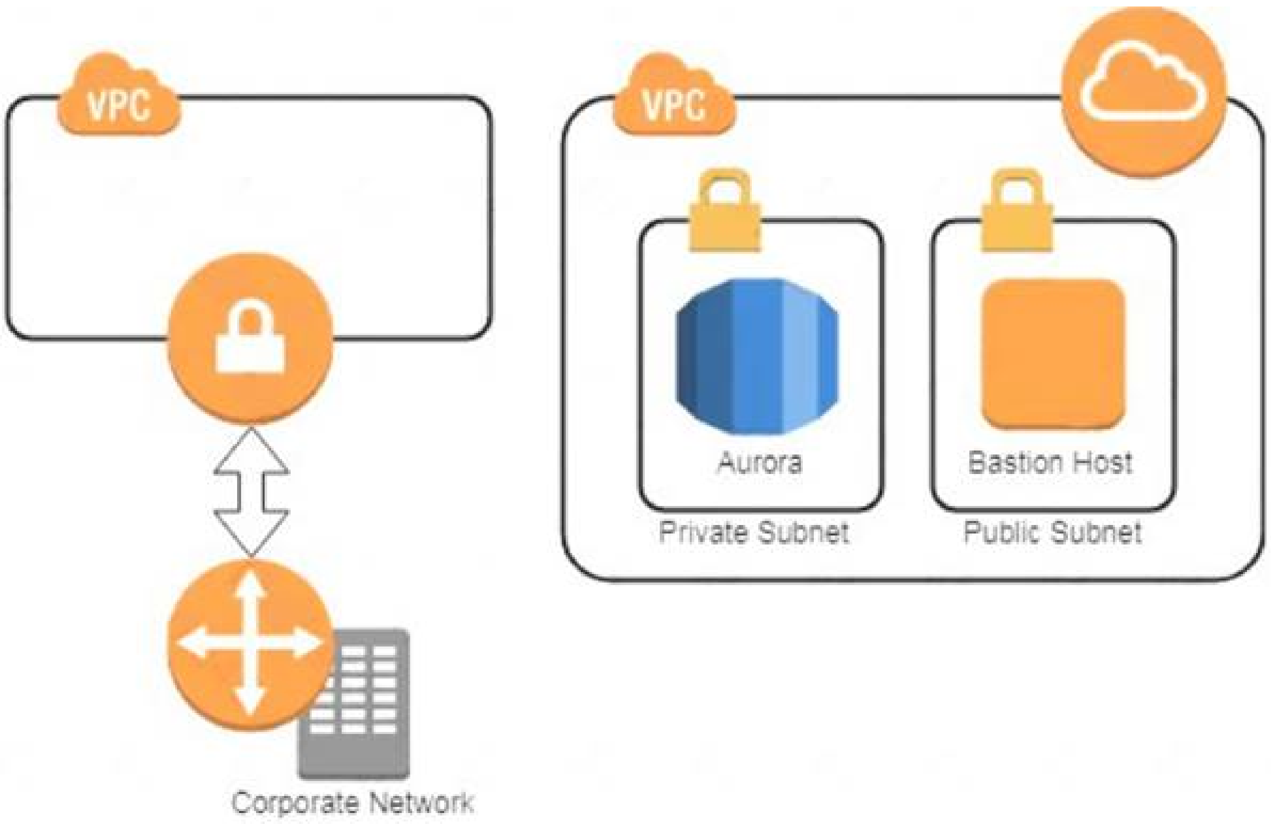
NEW QUESTION 223
- (Exam Topic 2)
A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old.
Which of the following options should the Security Engineer use?

A. In the AWS Console, choose the IAM service and select “Users”. Review the “Access Key Age” column.
B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
D. Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.

Answer: C

Explanation:
https://docs.aws.amazon.com/IAM/latest/APIReference/API_UpdateAccessKey.html
https://docs.aws.amazon.com/IAM/latest/APIReference/API_GenerateCredentialReport.html
https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetCredentialReport.html

NEW QUESTION 228
- (Exam Topic 2)
A company has two AWS accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private
subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.
How can a Security Engineer securely set up the bastion host?

A. Move the bastion host to the VPC with VPN connectivit
B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
C. Create a SSH port forwarding tunnel on the Developer’s workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
D. Move the bastion host to the VPC with VPN connectivit
E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
F. Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

Answer: A

NEW QUESTION 230
- (Exam Topic 2)
An organization has a system in AWS 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 AWS 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 235
- (Exam Topic 2)
Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

A. Stream the log files to a separate Cloudtrail trail
B. Stream the log files to a separate Cloudwatch Log group
C. Create an IAM policy that gives the desired level of access to the Cloudtrail trail
D. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group

Answer: BD

Explanation:
You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an IAM policy.
Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement
For more information on Log Groups and Log Streams, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Workinj
For more information on Access to Cloudwatch logs, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html
The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an IAM policy that gives the desired level of access to the Cloudwatch Log group
Submit your Feedback/Queries to our Experts

NEW QUESTION 240
- (Exam Topic 2)
A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.

An operational safety policy requires that access to specific credentials is independently auditable. What is the MOST cost-effective way to manage the storage of credentials?

A. Use AWS Systems Manager to store the credentials as Secure Strings Parameter
B. Secure by using an AWS KMS key.
C. Use AWS Key Management System to store a master key, which is used to encrypt the credential
D. The encrypted credentials are stored in an Amazon RDS instance.
E. Use AWS Secrets Manager to store the credentials.
F. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

Answer: A

Explanation:
https://docs.aws.amazon.com/systems-manager/latest/userguide/parameter-store-advanced-parameters.html

NEW QUESTION 245
- (Exam Topic 2)
A company has deployed a custom DNS server in AWS. The Security Engineer wants to ensure that Amazon EC2 instances cannot use the Amazon-provided DNS.
How can the Security Engineer block access to the Amazon-provided DNS in the VPC?

A. Deny access to the Amazon DNS IP within all security groups.
B. Add a rule to all network access control lists that deny access to the Amazon DNS IP.
C. Add a route to all route tables that black holes traffic to the Amazon DNS IP.
D. Disable DNS resolution within the VPC configuration.

Answer: D

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html

NEW QUESTION 247
- (Exam Topic 2)
Which of the following minimizes the potential attack surface for applications?

A. Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
B. Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific AWS resource.
C. Use AWS Direct Connect for secure trusted connections between EC2 instances within private subnets.
D. Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

Answer: A

Explanation:
https://aws.amazon.com/answers/networking/vpc-security-capabilities/ Security Group is stateful and hypervisor level.

NEW QUESTION 248
- (Exam Topic 2)
A company hosts a critical web application on the AWS Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?
Please select:

A. Consider using the AWS Shield Service
B. Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.
C. Consider using the AWS Shield Advanced Service
D. Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

Answer: C

Explanation:
Option A is invalid because the normal AWS Shield Service will not help in immediate action against a DDos attack. This can be done via the AWS Shield Advanced Service
Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDos attacks.
Option D is invalid because this is a logging service for AWS Services but cannot specifically protect against DDos attacks.
The AWS Documentation mentions the following
AWS Shield Advanced provides enhanced protections for your applications running on Amazon EC2. Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. AWS Shield Advanced is available to AWS Business Support and AWS Enterprise Support customers. AWS Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDoS attacks. AWS Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDoS Response Team (DRT) 24X7 to manage and mitigate their application layer DDoS attacks.
For more information on AWS Shield, please visit the below URL: https://aws.amazon.com/shield/faqs;
The correct answer is: Consider using the AWS Shield Advanced Service Submit your Feedback/Queries to our Experts

NEW QUESTION 252
- (Exam Topic 2)
A company runs an application on AWS 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 AWS Marketplace for users to connect to, and restrict workload access to traffic from that appliance.
D. Route all traffic to the workload through AWS WA
E. Add each employee’s home IP address into an AWS WAF rule, and block all other traffic.

Answer: C

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

NEW QUESTION 255
- (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 AWS resources that are encrypted by AWS KMS?

A. Copy the application’s AWS 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 AWS KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
C. Use AWS 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 AWS service to communicate with the source region’s AWS KMS so that it can decrypt the resource in the target region.

Answer: C

NEW QUESTION 260
- (Exam Topic 2)
An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.
How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

A. Use a filter in AWS CloudTrail to exclude the IP addresses of the Security team’s EC2 instances.
B. Add the Elastic IP addresses of the Security team’s EC2 instances to a trusted IP list in Amazon GuardDuty.
C. Install the Amazon Inspector agent on the EC2 instances that the Security team uses.
D. Grant the Security team’s EC2 instances a role with permissions to call Amazon GuardDuty API operations.

Answer: B

Explanation:
Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS 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 AWS account per region. Threat lists consist of known malicious IP addresses. GuardDuty generates findings based on threat lists. At any given time, you can have up to six uploaded threat lists per AWS account per region. https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

NEW QUESTION 261
- (Exam Topic 3)
Your company has a hybrid environment, with on-premise servers and servers hosted in the AWS cloud. They are planning to use the Systems Manager for patching servers. Which of the following is a pre-requisite for this to work;
Please select:

A. Ensure that the on-premise servers are running on Hyper-V.
B. Ensure that an IAM service role is created
C. Ensure that an IAM User is created
D. Ensure that an IAM Group is created for the on-premise servers

Answer: B

Explanation:
You need to ensure that an IAM service role is created for allowing the on-premise servers to communicate with the AWS Systems Manager.
Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that IAM users and groups are created For more information on the Systems Manager role please refer to the below URL: com/systems-rnanaeer/latest/usereuide/sysman-!
The correct answer is: Ensure that an IAM service role is created Submit your Feedback/Queries to our Experts

NEW QUESTION 262
- (Exam Topic 3)
A company has set up EC2 instances on the AW5 Cloud. There is a need to see all the IP addresses which are accessing the EC2 Instances. Which service can help achieve this?
Please select:

A. Use the AWS Inspector service
B. Use AWS VPC Flow Logs
C. Use Network ACL's
D. Use Security Groups

Answer: B

Explanation:

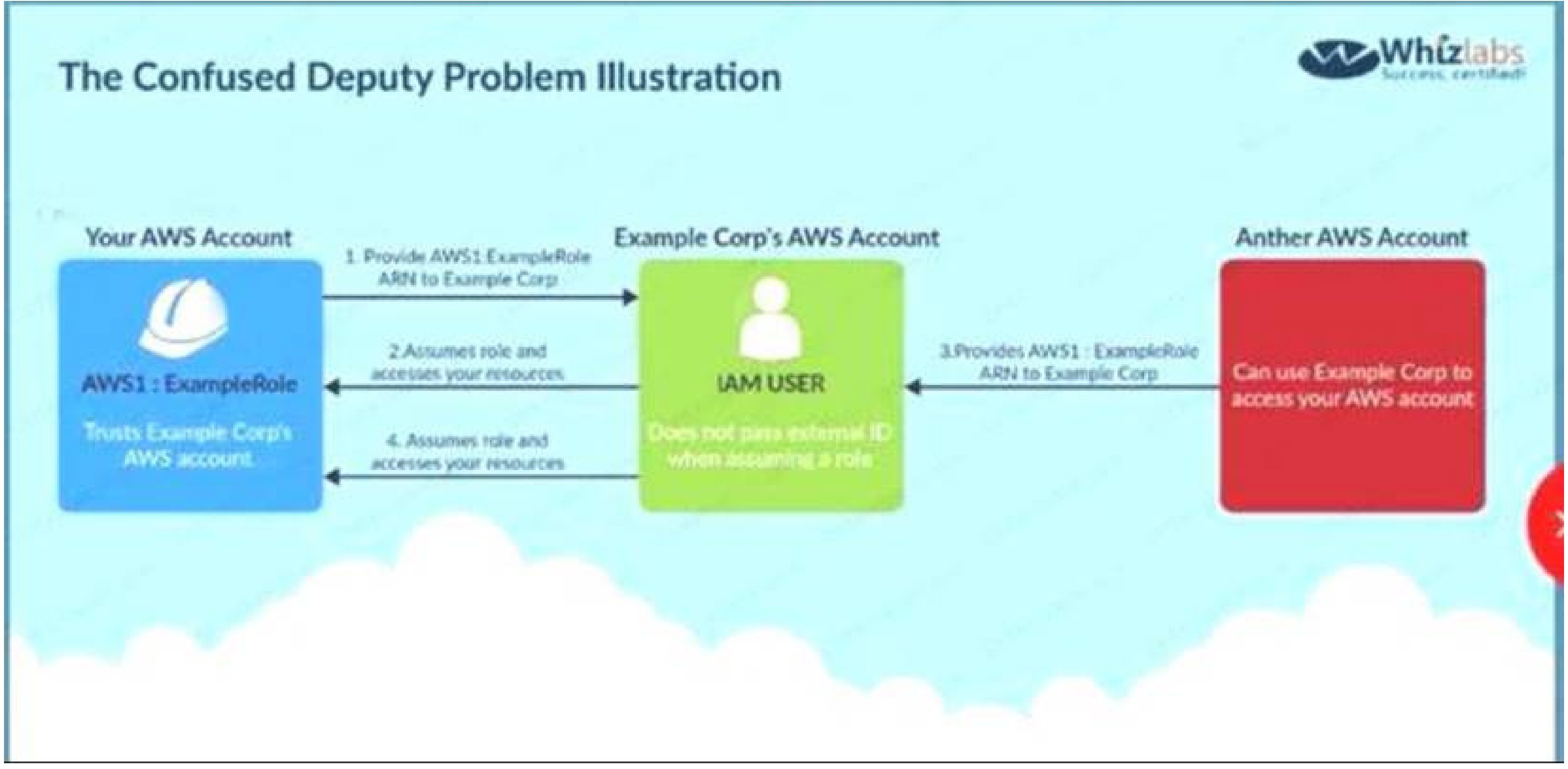
The AWS Documentation mentions the foil
A flow log record represents a network flow in your flow log. Each record captures the network flow for a specific 5-tuple, for a specific capture window. A 5-tuple is a set of five different values that specify the source, destination, and protocol for an internet protocol (IP) flow.
Options A,C and D are all invalid because these services/tools cannot be used to get the the IP addresses which are accessing the EC2 Instances
For more information on VPC Flow Logs please visit the URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html
The correct answer is: Use AWS VPC Flow Logs Submit vour Feedback/Queries to our Experts

NEW QUESTION 263
- (Exam Topic 3)
You currently have an S3 bucket hosted in an AWS Account. It holds information that needs be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.
Please select:

A. Ensure an IAM role is created which can be assumed by the partner account.
B. Ensure an IAM user is created which can be assumed by the partner account.
C. Ensure the partner uses an external id when making the request
D. Provide the ARN for the role to the partner account
E. Provide the Account Id to the partner account
F. Provide access keys for your account to the partner account

Answer: ACD

Explanation:
Option B is invalid because Roles are assumed and not IAM users
Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner
The below diagram from the AWS documentation showcases an example on this wherein an IAM role and external ID is us> access an AWS account resources
C:\Users\wk\Desktop\mudassar\Untitled.jpg


The Confused Deputy Problem Illustration
Whizlabs
Success, certified!
Your AWS Account
AWS1 : ExampleRole
Trusts Example Corp's AWS account
1. Provide AWS1 ExampleRole ARN to Example Corp
2.Assumes role and accesses your resources
4. Assumes role and accesses your resources
Example Corp's AWS Account
IAM USER
Does not pass external ID when assuming a role
3.Provides AWS1 : ExampleRole ARN to Example Corp
Anther AWS Account
Can use Example Corp to access your AWS account

For more information on creating roles for external ID'S please visit the following URL:
The correct answers are: Ensure an IAM role is created which can be assumed by the partner account. Ensure the partner uses an external id when making the request Provide the ARN for the role to the partner account
Submit your Feedback/Queries to our Experts

NEW QUESTION 268
- (Exam Topic 3)
Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws. Which of the following can be done to ensure this? Choose 2 answers from the options given below.
Please select:

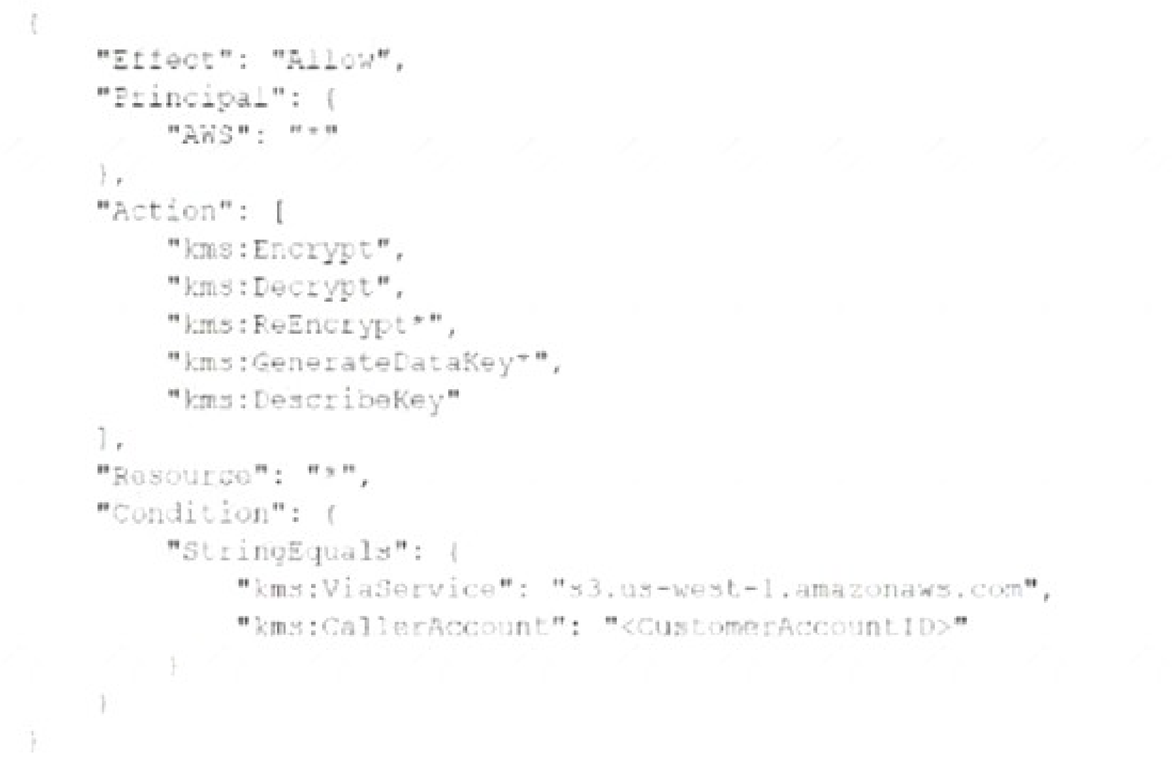
A. Use AWS Config to ensure that the servers have no critical flaws.
B. Use AWS inspector to ensure that the servers have no critical flaws.
C. Use AWS inspector to patch the servers
D. Use AWS SSM to patch the servers

Answer: BD

Explanation:
The AWS Documentation mentions the following on AWS Inspector
Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.
Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers Option C is invalid because the AWS Inspector service is not used to patch servers
For more information on AWS Inspector, please visit the following URL: https://aws.amazon.com/inspector>
Once you understand the list of servers which require critical updates, you can rectify them by installing the required patches via the SSM tool.
For more information on the Systems Manager, please visit the following URL: https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html

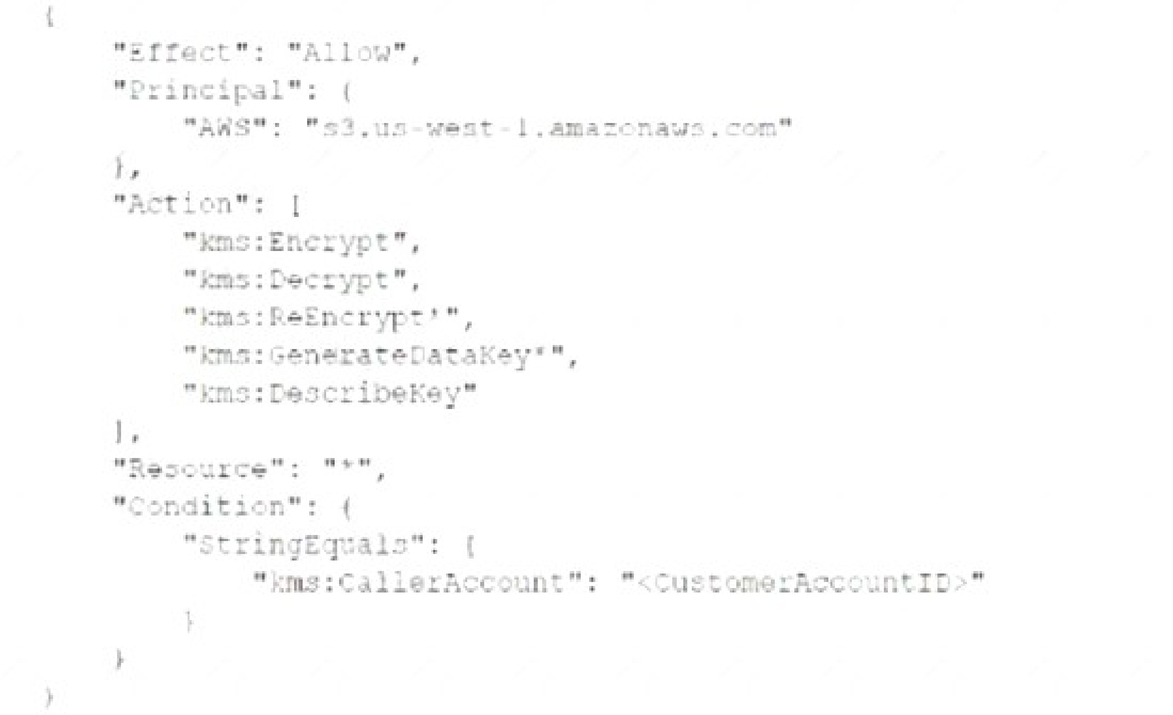
The correct answers are: Use AWS Inspector to ensure that the servers have no critical flaws.. Use AWS SSM to patch the servers
(

NEW QUESTION 269
- (Exam Topic 3)
A security engineer needs to create an AWS Key Management Service <AWS KMS) key that will De used to encrypt all data stored in a company's Amazon S3 Buckets in the us-west-1 Region. The key will use
server-side encryption. Usage of the key must be limited to requests coming from Amazon S3 within the company's account.
Which statement in the KMS key policy will meet these requirements?
A)



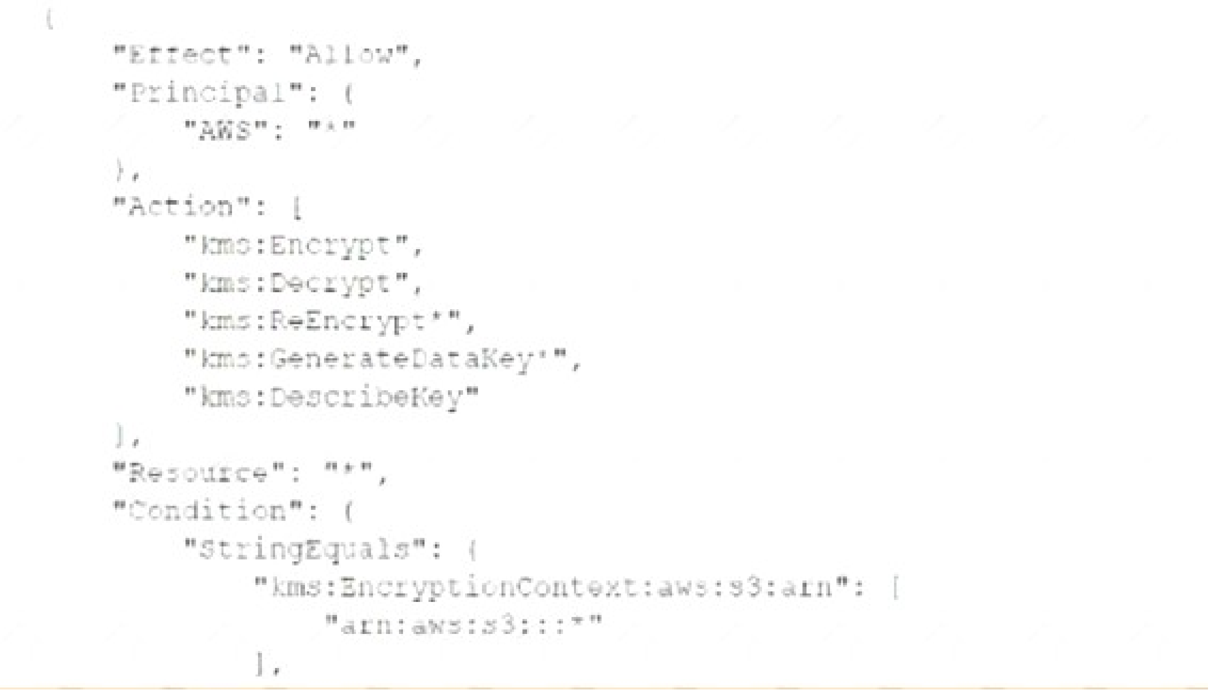
```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "s3.us-west-1.amazonaws.com",
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

B)



```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "s3.us-west-1.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

C)



```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::*"
            ],
```

A. Option A
B. Option B

C. Option C

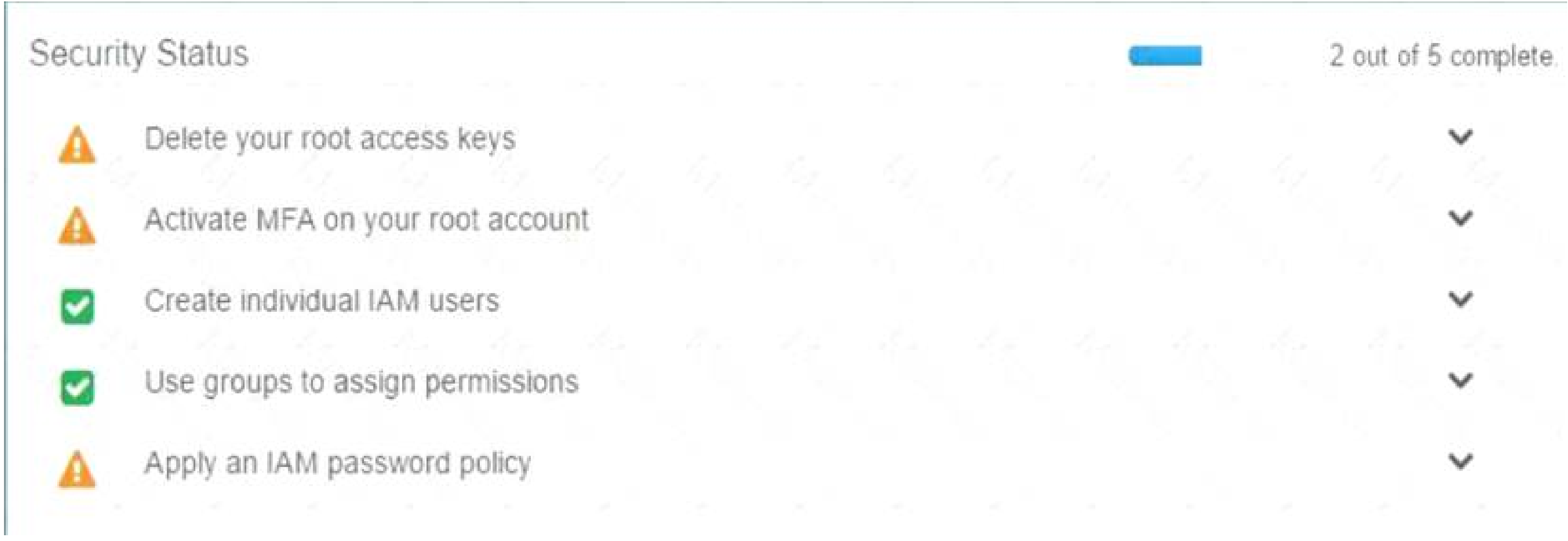
Answer: C

NEW QUESTION 271
- (Exam Topic 3)
Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which three IAM best practices should you consider implementing?
Please select:

A. Create individual IAM users
B. Configure MFA on the root account and for privileged IAM users
C. Assign IAM users and groups configured with policies granting least privilege access
D. Ensure all users have been assigned and dre frequently rotating a password, access ID/secret key, andX.509 certificate

Answer: ABC

Explanation:
When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.
C:\Users\wk\Desktop\mudassar\Untitled.jpg



Security Status — 2 out of 5 complete

⚠ Delete your root access keys
⚠ Activate MFA on your root account
✓ Create individual IAM users
✓ Use groups to assign permissions
⚠ Apply an IAM password policy

Option D is invalid because as per the dashboard, this is not part of the security recommendation For more information on best security practices please visit the URL:
https://aws.amazon.com/whitepapers/aws-security-best-practices;
The correct answers are: Create individual IAM users, Configure MFA on the root account and for privileged IAM users. Assign IAM users and groups configured with policies granting least privilege access
Submit your Feedback/Queries to our Experts

NEW QUESTION 272
- (Exam Topic 3)
A development team is using an AWS Key Management Service (AWS KMS) CMK to try to encrypt and decrypt a secure string parameter from AWS Systems Manager Parameter Store. However, the development team receives an error message on each attempt.
Which issues that are related to the CMK could be reasons for the error? (Select TWO.)

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

Answer: AD

NEW QUESTION 277
- (Exam Topic 3)
A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.
Please select:

A. Enable CloudTrail logging in all accounts into S3 buckets
B. Enable CloudTrail logging in all accounts into Amazon Glacier
C. Ensure a lifecycle policy is defined on the S3 bucket to move the data to EBS volumes after 6 months.
D. Ensure a lifecycle policy is defined on the S3 bucket to move the data to Amazon Glacier after 6 months.

Answer: AD

Explanation:
Cloudtrail publishes the trail of API logs to an S3 bucket
Option B is invalid because you cannot put the logs into Glacier from CloudTrail
Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes For more information on Cloudtrail logging, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/cloudtrail-find-log-files.htmll
You can then use Lifecycle policies to transfer data to Amazon Glacier after 6 months For more information on S3 lifecycle policies, please visit the below URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

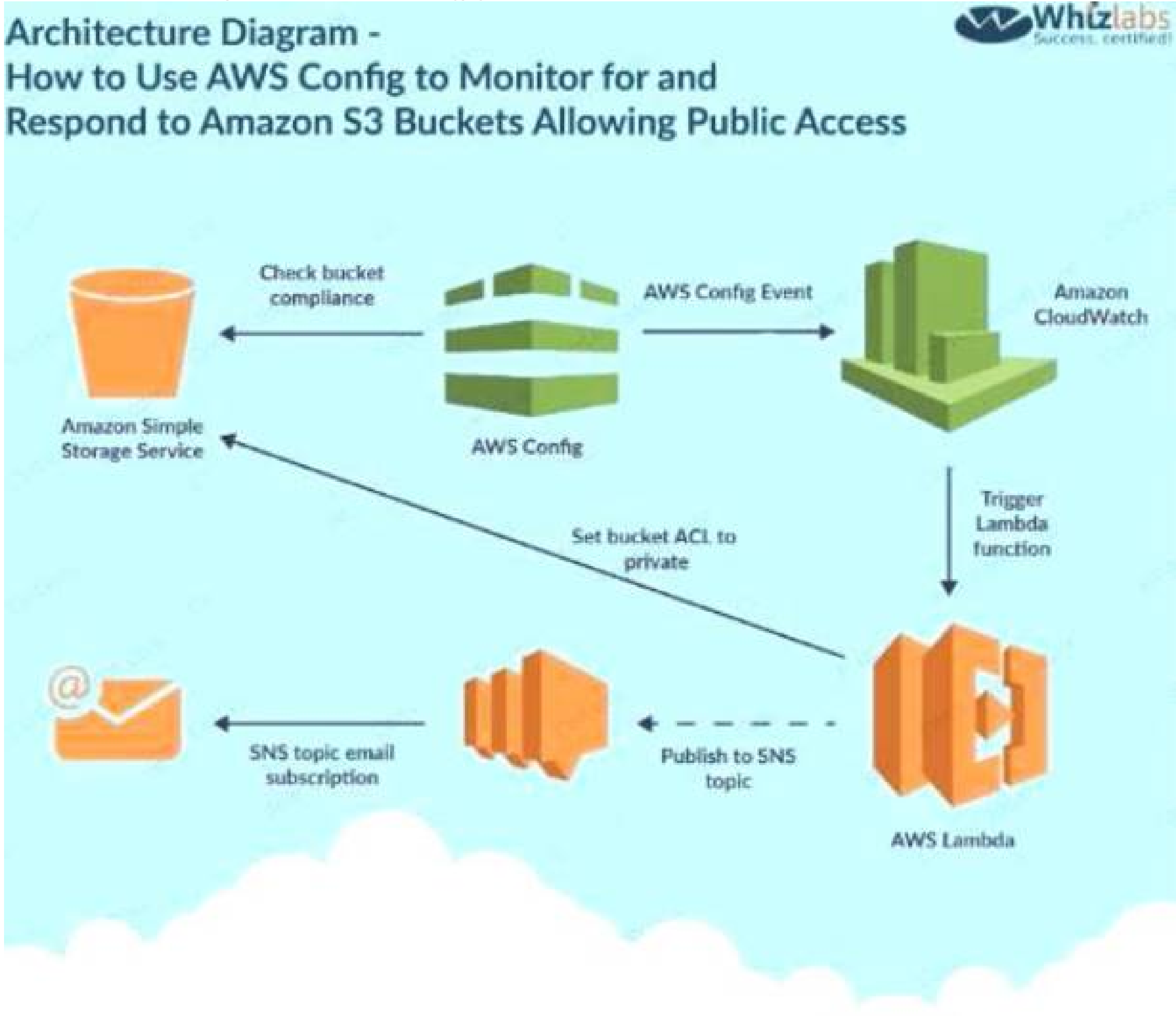
The correct answers are: Enable CloudTrail logging in all accounts into S3 buckets. Ensure a lifecycle policy is defined on the bucket to move the data to Amazon Glacier after 6 months.
Submit your Feedback/Queries to our Experts

NEW QUESTION 282
- (Exam Topic 3)
A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private. How can this be ensured continually? Choose 2 answers from the options given below
Please select:

A. Use AWS Config to monitor changes to the AWS Bucket
B. Use AWS Lambda function to change the bucket policy
C. Use AWS Trusted Advisor API to monitor the changes to the AWS Bucket
D. Use AWS Lambda function to change the bucket ACL

Answer: AD

Explanation:
One of the AWS Blogs mentions the usage of AWS Config and Lambda to achieve this. Below is the diagram representation of this
C:\Users\wk\Desktop\mudassar\Untitled.jpg


Architecture Diagram -
How to Use AWS Config to Monitor for and
Respond to Amazon S3 Buckets Allowing Public Access
Whizlabs
Success. certified!
Check bucket compliance
AWS Config Event
Amazon CloudWatch
Amazon Simple Storage Service
AWS Config
Trigger Lambda function
Set bucket ACL to private
SNS topic email subscription
Publish to SNS topic
AWS Lambda

ption C is invalid because the Trusted Advisor API cannot be used to monitor changes to the AWS Bucket Option B doesn't seems to be the most appropriate.
* 1. If the object is in a bucket in which all the objects need to be private and the object is not private anymore, the Lambda function makes a PutObjectAcl call to S3 to make the object private.
|https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-a The following link also specifies that
Create a new Lambda function to examine an Amazon S3 buckets ACL and bucket policy. If the bucket ACL is found to al public access, the Lambda function overwrites it to be private. If a bucket policy is found, the Lambda function creatt an SNS message, puts the policy in the message body, and publishes it to the Amazon SNS topic we created. Bucket policies can be complex, and overwriting your policy may cause unexpected loss of access, so this Lambda function doesn't attempt to alter your policy in any way.
https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucke Based on these facts Option D seems to be more appropriate then Option B.
For more information on implementation of this use case, please refer to the Link: https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-bucke
The correct answers are: Use AWS Config to monitor changes to the AWS Bucket Use AWS Lambda function to change the bucket ACL

NEW QUESTION 284
- (Exam Topic 3)
An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?
Please select:

A. Launch the test and production instances in separate regions and allow region wise access to the group
B. Define the IAM policy which allows access based on the instance ID
C. Create an IAM policy with a condition which allows access to only small instances
D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specification tags

Answer: D

Explanation:

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it
Option A is invalid because this is not a recommended practices
Option B is invalid because this is an overhead to maintain this in policies Option C is invalid because the instance type will not resolve the requirement For information on resource tagging, please visit the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usine_Tags.htmll
The correct answer is: Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags
Submit your Feedback/Queries to our Experts

NEW QUESTION 287
- (Exam Topic 3)
An organization must establish the ability to delete an AWS KMS Customer Master Key (CMK) within a
24- hour timeframe to keep it from being used for encrypt or decrypt operations Which of tne following actions will address this requirement?

A. Manually rotate a key within KMS to create a new CMK immediately
B. Use the KMS import key functionality to execute a delete key operation
C. Use the schedule key deletion function within KMS to specify the minimum wait period for deletion
D. Change the KMS CMK alias to immediately prevent any services from using the CMK.

Answer: C

NEW QUESTION 289
- (Exam Topic 3)
A company wants to ensure that its AWS resources can be launched only in the us-east-1 and us-west-2 Regions.
What is the MOST operationally efficient solution that will prevent developers from launching Amazon EC2 instances in other Regions?

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

Answer: C

NEW QUESTION 292
- (Exam Topic 3)
Your company makes use of S3 buckets for storing data. There is a company policy that all services should have logging enabled. How can you ensure that logging is always enabled for created S3 buckets in the AWS Account?
Please select:

A. Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
B. Use AWS Config Rules to check whether logging is enabled for buckets
C. Use AWS Cloudwatch metrics to check whether logging is enabled for buckets
D. Use AWS Cloudwatch logs to check whether logging is enabled for buckets

Answer: B

Explanation:
This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers Example rule with configuration change trigger
* 1. You add the AWS Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
* 2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
* 3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.
Option A is invalid because AWS Inspector cannot be used to scan all buckets
Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets. For more information on Config Rules please see the below Link:
> https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
The correct answer is: Use AWS Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 296
- (Exam Topic 3)
A company's AWS account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?
Please select:

A. Create a new role and add each user to the IAM role
B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
C. Create a policy and apply it to multiple users using a JSON script
D. Create an S3 bucket policy with unlimited access which includes each user's AWS account ID

Answer: B

Explanation:
Option A is incorrect since you don't add a user to the IAM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach
An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you

change the permissions on the group scale, it will affect all the users in that group
For more information on IAM Groups, just browse to the below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
Submit your Feedback/Queries to our Experts

NEW QUESTION 298
- (Exam Topic 3)
A company deployed AWS Organizations to help manage its increasing number of AWS accounts. A security engineer wants to ensure only principals in the Organization structure can access a specic Amazon S3 bucket. The solution must also minimize operational overhead
Which solution will meet these requirements?

A. 1 Put all users into an IAM group with an access policy granting access to the J bucket.
B. Have the account creation trigger an AWS Lambda function that manages the bucket policy, allowing access to accounts listed in the policy only.
C. Add an SCP to the Organizations master account, allowing all principals access to the bucket.
D. Specify the organization ID in the global key condition element of a bucket policy, allowing all principals access.

Answer: D

NEW QUESTION 300
- (Exam Topic 3)
Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below
Please select:

A. Create an IAM user in the company account
B. Create an IAM Role in the company account
C. Ensure the IAM user has access for read-only to the S3 buckets
D. Ensure the IAM Role has access for read-only to the S3 buckets

Answer: BD

Explanation:
The AWS Documentation mentions the following
To share log files between multiple AWS accounts, you must perform the following general steps. These steps are explained in detail later in this section.
Create an IAM role for each account that you want to share log files with.
For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.
Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files. Options A and C are invalid because creating an IAM user and then sharing the IAM user credentials with the vendor is a direct 'NO' practise from a security perspective.
For more information on sharing cloudtrail logs files, please visit the following URL https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-sharine-loes.htmll
The correct answers are: Create an IAM Role in the company account Ensure the IAM Role has access for read-only to the S3 buckets
Submit your Feedback/Queries to our Experts

NEW QUESTION 305
- (Exam Topic 3)
Your company is planning on developing an application in AWS. This is a web based application. The application user will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.
Please select:

A. Create an OlDC identity provider in AWS
B. Create a SAML provider in AWS
C. Use AWS Cognito to manage the user profiles
D. Use IAM users to manage the user profiles

Answer: C

Explanation:
The AWS Documentation mentions the following
A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.
User pools provide:
Sign-up and sign-in services.
A built-in, customizable web Ul to sign in users.
Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.
User directory management and user profiles.
Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
Customized workflows and user migration through AWS Lambda triggers. Options A and B are invalid because these are not used to manage users Option D is invalid because this would be a maintenance overhead
For more information on Cognito User Identity pools, please refer to the below Link: https://docs.aws.amazon.com/coenito/latest/developerguide/cognito-user-identity-pools.html
The correct answer is: Use AWS Cognito to manage the user profiles Submit your Feedback/Queries to our Experts

NEW QUESTION 310
......