Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/

NEW QUESTION 1

You are designing a custom 1AM 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.
```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
   ],
  "Resource": "Resource": "arn:aws:s3:::*",
  "Condition": {
    "Bool": {"aws:MultiFactorAuthPresent": true}
  }
 }
}
```

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

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

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

A.

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

A. Create a VPC endpoint for DynamoDB within a VP
B. Configure the Lambda function to access resources in the VPC.
C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB tabl
D. Attach the poll to the DynamoDB table.
E. Create an 1AM user with permissions to write to the DynamoDB tabl
F. Store an access key for that user in the Lambda environment variables.
G. Create an 1AM service role with permissions to write to the DynamoDB tabl
H. Associate that role with the Lambda function.

Answer: D

Explanation:
The ideal way is to create an 1AM role which has the required permissions and then associate it with the Lambda function
The AWS Documentation additionally mentions the following
Each Lambda function has an 1AM role (execution role) associated with it. You specify the 1AM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the 1AM role:
If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role.
If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role.
Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB
Option B is invalid because resources policies are present for resources such as S3 and KMS, but not AWS Lambda
Option C is invalid because AWS Roles should be used and not 1AM Users
For more information on the Lambda permission model, please visit the below URL: https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Create an 1AM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.
Submit your Feedback/Queries to our Exp

NEW QUESTION 3
You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.
Please select:

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

Answer: AB

Explanation:
The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.
The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration
Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.htmll
The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123
Submit your Feedback/Queries to our Experts

NEW QUESTION 4
You have just received an email from AWS Support stating that your AWS account might have been compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.
Please select:

A. Change the root account password.
B. Rotate all 1AM access keys
C. Keep all resources running to avoid disruption
D. Change the password for all 1AM user

Answer: ABD

Explanation:
One of the articles from AWS mentions what should be done in such a scenario
If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the

following tasks:

Change your AWS root account password and the passwords of any 1AM users. Delete or rotate all root and AWS Identity and Access Management (1AM) access keys.

Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or 1AM users.

Respond to any notifications you received from AWS Support through the AWS Support Center. Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.

For more information on the article, please visit the below URL: https://aws.amazon.com/premiumsupport/knowledee-center/potential-account-compromise>

The correct answers are: Change the root account password. Rotate all 1AM access keys. Change the password for all 1AM users. Submit your Feedback/Queries to our Experts

NEW QUESTION 5

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 6

You have setup a set of applications across 2 VPC's. You have also setup VPC Peering. The applications are still not able to communicate across the Peering connection. Which network troubleshooting steps should be taken to resolve the issue?
Please select:

A. Ensure the applications are hosted in a public subnet
B. Check to see if the VPC has an Internet gateway attached.
C. Check to see if the VPC has a NAT gateway attached.
D. Check the Route tables for the VPC's

Answer: D

Explanation:

After the VPC peering connection is established, you need to ensure that the route tables are modified to ensure traffic can between the VPCs

Option A ,B and C are invalid because allowing access the Internet gateway and usage of public subnets can help for Inter, access, but not for VPC Peering.

For more information on VPC peering routing, please visit the below URL:

.com/AmazonVPC/latest/Peeri

The correct answer is: Check the Route tables for the VPCs Submit your Feedback/Queries to our Experts

NEW QUESTION 7

You need to ensure that objects in an S3 bucket are available in another region. This is because of the criticality of the data that is hosted in the S3 bucket. How can you achieve this in the easiest way possible?
Please select:

A. Enable cross region replication for the bucket
B. Write a script to copy the objects to another bucket in the destination region
C. Create an S3 snapshot in the destination region
D. Enable versioning which will copy the objects to the destination region

Answer: A

Explanation:

Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3

Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following

Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different AWS Regions.

For more information on Cross region replication in the Simple Storage Service, please visit the below URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html

The correct answer is: Enable cross region replication for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 8

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 9
You have a set of Keys defined using the AWS KMS service. You want to stop using a couple of keys , but are not sure of which services are currently using the keys. Which of the following would be a
safe option to stop using the keys from further usage. Please select:

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

Answer: B

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

NEW QUESTION 10
You are building a large-scale confidential documentation web server on AWSand all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below
Please select:

A. Create an Identity and Access Management (1AM) user for CloudFront and grant access to the objects in your S3 bucket to that 1AM User.
B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: B

Explanation:
If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront ace logs are less useful because they're incomplete.
Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an 1AM user
Option C and D are invalid because using policies will not help fulfil the requirement For more information on Origin Access Identity please see the below Link:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contentrestrictine- access-to-s3.htmll
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
(
Submit your Feedback/Queries to our Experts

NEW QUESTION 10
A security engineer must ensure that all infrastructure launched in the company AWS account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AM Is and that all attached EBS volumes are encrypted. Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2 answers from the options given below.
Please select:

A. Set up a CloudWatch event based on Trusted Advisor metrics
B. Trigger a Lambda function from a scheduled CloudWatch event that terminates non-compliant infrastructure.
C. Set up a CloudWatch event based on Amazon inspector findings
D. Monitor compliance with AWS Config Rules triggered by configuration changes
E. Trigger a CLI command from a CloudWatch event that terminates the infrastructure

Answer: BD

Explanation:
You can use AWS Config to monitor for such Event
Option A is invalid because you cannot set Cloudwatch events based on Trusted Advisor checks.
Option C is invalid Amazon inspector cannot be used to check whether instances are launched from a specific A
Option E is invalid because triggering a CLI command is not the preferred option, instead you should use Lambda functions for all automation purposes.
For more information on Config Rules please see the below Link: https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
These events can then trigger a lambda function to terminate instances For more information on Cloudwatch events please see the below Link:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.
(
The correct answers are: Trigger a Lambda function from a scheduled Cloudwatch event that terminates non-compliant infrastructure., Monitor compliance with AWS Config Rules triggered by configuration changes
Submit your Feedback/Queries to our Experts

NEW QUESTION 11
A company hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?
Please select:

A. Use Bucket policies
B. Use the Secure Token service
C. Use 1AM user policies
D. Use AWS Access Keys

Answer: AC

Explanation:
The AWS Documentation mentions the following
Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as
resource-based policies. For example, bucket policies and access control lists (ACLs) are resourcebased policies. You can also attach access policies to users in your account. These are called user
policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.
Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below
Link: https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.htmll
The correct answers are: Use Bucket policies. Use 1AM user policies Submit your Feedback/Queries to our Experts

NEW QUESTION 15
You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below Please select:

A. Amazon Cloudwatch Logs
B. Amazon VPC Flow Logs
C. Amazon AWS Config
D. Amazon Cloudtrail

Answer: AD

Explanation:
The AWS Documentation mentions the following about these services
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.
Option B is incorrect because VPC flow logs can only check for flow to instances in a VPC Option C is incorrect because this can check for configuration changes only
For more information on Cloudtrail, please refer to below URL: https://aws.amazon.com/cloudtrail;
You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs.
For more information on Cloudwatch logs, please refer to below URL: http://docs.aws.amazon.com/AmazonCloudWatch/latest/loes/WhatisCloudWatchLoES.htmll
The correct answers are: Amazon Cloudwatch Logs, Amazon Cloudtrail

NEW QUESTION 18
A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working. What is the other step that needs to be followed to ensure that the AD domain join can work as intended
Please select:

A. Change the VPC peering connection to a VPN connection
B. Change the VPC peering connection to a Direct Connect connection
C. Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets
D. Ensure that the AD is placed in a public subnet

Answer: C

Explanation:
In addition to VPC peering and setting the right route tables, the security groups for the AD EC2 instance needs to ensure the right rules are put in place for allowing incoming traffic.
Option A and B is invalid because changing the connection type will not help. This is a problem with the Security Groups.
Option D is invalid since the AD should not be placed in a public subnet
For more information on allowing ingress traffic for AD, please visit the following url
|https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html|

The correct answer is: Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets Submit your Feedback/Queries to our Experts

NEW QUESTION 23
A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition , it should be ensured that objects are available in a secondary region if the primary one goes down. Which of the following can help fulfil these requirements? Choose 2 answers from the options given below
Please select:

A. Enable bucket versioning and also enable CRR
B. Enable bucket versioning and enable Master Pays
C. For the Bucket policy add a condition for {"Null": {"aws:MultiFactorAuthAge": true}}
D. Enable the Bucket ACL and add a condition for {"Null": {"aws:MultiFactorAuthAge": true}}

Answer: AC

Explanation:
The AWS Documentation mentions the following Adding a Bucket Policy to Require MFA
Amazon S3 supports MFA-protected API access, a feature that can enforce multi-factor authentication (MFA) for access to your Amazon S3 resources. Multi-factor authentication provides an extra level of security you can apply to your AWS environment. It is a security feature that requires users to prove physical possession of an MFA device by providing a valid MFA code. For more information, go to AWS Multi-Factor Authentication. You can require MFA authentication for any requests to access your Amazoi. S3 resources.
You can enforce the MFA authentication requirement using the aws:MultiFactorAuthAge key in a bucket policy. 1AM users car access Amazon S3 resources by using temporary credentials issued by
the AWS Security Token Service (STS). You provide the MFA code at the time of the STS request. When Amazon S3 receives a request with MFA authentication, the aws:MultiFactorAuthAge key provides a numeric value indicating how long ago (in seconds) the temporary credential was created. If the temporary credential provided in the request was not created using an MFA device, this key value is null (absent). In a bucket policy, you can add a condition to check this value, as shown in the following example bucket policy. The policy denies any Amazon S3 operation on the /taxdocuments folder in the examplebucket bucket if the request is not MFA authenticated. To learn more about MFA authentication, see Using Multi-Factor Authentication (MFA) in AWS in the 1AM User Guide.

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/taxdocuments/*",
      "Condition": { "Null": { "aws:MultiFactorAuthAge": true }}
    }
  ]
}
```

Option B is invalid because just enabling bucket versioning will not guarantee replication of objects Option D is invalid because the condition for the bucket policy needs to be set accordingly For more information on example bucket policies, please visit the following URL: •
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
Also versioning and Cross Region replication can ensure that objects will be available in the destination region in case the primary region fails.
For more information on CRR, please visit the following URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html
The correct answers are: Enable bucket versioning and also enable CRR, For the Bucket policy add a condition for {"Null": { "aws:MultiFactorAuthAge": true}}
Submit your Feedback/Queries to our Experts

NEW QUESTION 24
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 28
You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.
Please select:

A. Check to see if the right role has been assigned to the EC2 instances
B. Check to see if the 1AM user has the right permissions for EC2
C. Ensure that agent is running on the instances.
D. Check the Instance status by using the Health AP

Answer: ACD

Explanation:
For ensuring that the instances are configured properly you need to ensure the followi .
1) You installed the latest version of the SSM Agent on your instance
2) Your instance is configured with an AWS Identity and Access Management (1AM) role that enables the instance to communicate with the Systems Manager API
3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances The status of one or more instances
The last time the instance sent a heartbeat value The version of the SSM Agent
The operating system
The version of the EC2Config service (Windows) The status of the EC2Config service (Windows)
Option B is invalid because 1AM users are not supposed to be directly granted permissions to EC2 Instances For more information on troubleshooting AWS SSM, please visit the following URL: https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remotecommands. html
The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.
Submit your Feedback/Queries to our Experts

NEW QUESTION 30
A company has an existing AWS account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.
Please select:

A. Change the access keys for all 1AM users.
B. Delete all custom created 1AM policies
C. Delete the access keys for the root account
D. Confirm MFAtoa secure device
E. Change the password for the root account
F. Change the password for all 1AM users

Answer: CDE

Explanation:
Now if the root account has a chance to be compromised, then you have to carry out the below steps
1. Delete the access keys for the root account
2. Confirm MFA to a secure device
3. Change the password for the root account
This will ensure the employee who has left has no change to compromise the resources in AWS. Option A is invalid because this would hamper the working of the current IAM users
Option B is invalid because this could hamper the current working of services in your AWS account Option F is invalid because this would hamper the working of the current IAM users
For more information on IAM root user, please visit the following URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id root-user.html
The correct answers are: Delete the access keys for the root account Confirm MFA to a secure device. Change the password for the root account
Submit Your Feedback/Queries to our Experts

NEW QUESTION 32
A company had developed an incident response plan 18 months ago. Regular implementations of the response plan are carried out. No changes have been made to the response plan have been made since its creation. Which of the following is a right statement with regards to the plan?
Please select:

A. It places too much emphasis on already implemented security controls.
B. The response plan is not implemented on a regular basis
C. The response plan does not cater to new services
D. The response plan is complete in its entirety

Answer: C

Explanation:
So definitely the case here is that the incident response plan is not catering to newly created services. AWS keeps on changing and adding new services and hence the response plan must cater to these new services.
Option A and B are invalid because we don't know this for a fact.
Option D is invalid because we know that the response plan is not complete, because it does not cater to new features of AWS
For more information on incident response plan please visit the following URL: https://aws.amazon.com/blogs/publicsector/buildins-a-cloud-specific-incident-response-plan; The correct answer is: The response plan does not cater to new services Submit your Feedback/Queries to our Experts

NEW QUESTION 33
An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users. Which of the following is a secure way of ensuring that the EC2 Instance access the Dynamo table
Please select:

A. Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance
B. Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
C. Use 1AM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
D. Use 1AM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance

Answer: A

Explanation:
To always ensure secure access to AWS resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to AWS services. Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to AWS services. Option D is invalid because there is no way access groups can be assigned to EC2 Instances. For more information on 1AM Roles, please refer to the below URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id roles.html
The correct answer is: Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 35
A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database. How can this be achieved?
Please select:

A. Encrypt the EBS volumes of the underlying EC2 Instances
B. Use AWS KMS Customer Default master key
C. Use SSL/TLS for encrypting the data
D. Use S3 Encryption

Answer: B

Explanation:
The AWS Documentation mentions the following
Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either
AWS Key Management Servic (AWS KMS) or a hardware security module (HSM) to manage the toplevel
encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.
Option A is invalid because its the cluster that needs to be encrypted
Option C is invalid because this encrypts objects in transit and not objects at rest Option D is invalid because this is used only for objects in S3 buckets
For more information on Redshift encryption, please visit the following URL: https://docs.aws.amazon.com/redshift/latest/memt/workine-with-db-encryption.htmll
The correct answer is: Use AWS KMS Customer Default master key Submit your Feedback/Queries to our Experts

NEW QUESTION 39
A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions. The audit needs to be applied for future regions as well. Which of the following can be used to fulfil this requirement.
Please select:

A. Ensure Cloudtrail for each regio
B. Then enable for each future region.
C. Ensure one Cloudtrail trail is enabled for all regions.
D. Create a Cloudtrail for each regio
E. Use Cloudformation to enable the trail for all future regions.
F. Create a Cloudtrail for each regio
G. Use AWS Config to enable the trail for all future region

Answer: B

Explanation:
The AWS Documentation mentions the following
You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result you will receive log files containing API activity for the new region without taking any action.
Option A and C is invalid because this would be a maintenance overhead to enable cloudtrail for every region
Option D is invalid because this AWS Config cannot be used to enable trails For more information on this feature, please visit the following URL:
https://aws.ama2on.com/about-aws/whats-new/20l5/l2/turn-on-cloudtrail-across-all-reeions-andsupport- for-multiple-trails
The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

NEW QUESTION 43
Your company hosts critical data in an S3 bucket. There is a requirement to ensure that all data is encrypted. There is also metadata about the information stored in the bucket that needs to be encrypted as well. Which of the below measures would you take to ensure that the metadata is encrypted?
Please select:

A. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server side encryption.
B. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server KMS encryption.
C. Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time.
D. Put thp metadata in thp S3 hurkpf itsel

Answer: C

Explanation:
Option A ,B and D are all invalid because the metadata will not be encrypted in any case and this is a key requirement from the question.
One key thing to note is that when the S3 bucket objects are encrypted, the meta data is not encrypted. So the best option is to use an encrypted DynamoDB table
Important
All GET and PUT requests for an object protected by AWS KMS will fail if they are not made via SSL or by using SigV4. SSE-KMS encrypts only the object dat
A. Any object metadata is not encrypted. For
more information on using KMS encryption for S3, please refer to below URL: 1 https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html
The correct answer is: Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time. Submit your Feedback/Queries to our Experts

NEW QUESTION 46
One of your company's EC2 Instances have been compromised. The company has strict po thorough investigation on finding the culprit for the security breach.
What would you do in from the options given below.
Please select:

A. Take a snapshot of the EBS volume
B. Isolate the machine from the network
C. Make sure that logs are stored securely for auditing and troubleshooting purpose
D. Ensure all passwords for all 1AM users are changed
E. Ensure that all access kevs are rotate

Answer: ABC

Explanation:
Some of the important aspects in such a situation are
1) First isolate the instance so that no further security harm can occur on other AWS resources
2) Take a snapshot of the EBS volume for further investigation. This is incase if you need to shutdown the initial instance and do a separate investigation on the data
3) Next is Option C. This indicates that we have already got logs and we need to make sure that it is stored securely so that n unauthorised person can access it and manipulate it.
Option D and E are invalid because they could have adverse effects for the other 1AM users. For more information on adopting a security framework, please refer to below URL https://d1 .awsstatic.com/whitepapers/compliance/NIST Cybersecurity Framework
Note:
In the question we have been asked to take actions to find the culprit and to help the investigation or to further reduce the damage that has happened due to the security breach. So by keeping logs secure is one way of helping the investigation.
The correct answers are: Take a snapshot of the EBS volume. Isolate the machine from the network. Make sure that logs are stored securely for auditing and troubleshooting purpose
Submit your Feedback/Queries to our Experts

NEW QUESTION 51
Your company hosts a large section of EC2 instances in AWS. There are strict security rules governing the EC2 Instances. During a potential security breach , you need to ensure quick investigation of the underlying EC2 Instance. Which of the following service can help you quickly provision a test environment to look into the breached instance.
Please select:

A. AWS Cloudwatch
B. AWS Cloudformation
C. AWS Cloudtrail
D. AWS Config

Answer: B

Explanation:
The AWS Security best practises mentions the following
Unique to AWS, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can preconfigure instances in an isolated environment that contains all the necessary tools forensic teams
need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean room. Option A is incorrect since this is a logging service and cannot be used to provision a test environment
Option C is incorrect since this is an API logging service and cannot be used to provision a test environment
Option D is incorrect since this is a configuration service and cannot be used to provision a test environment
For more information on AWS Security best practises, please refer to below URL: https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pd1
The correct answer is: AWS Cloudformation Submit your Feedback/Queries to our Experts

NEW QUESTION 56
Which of the following is the responsibility of the customer? Choose 2 answers from the options given below.
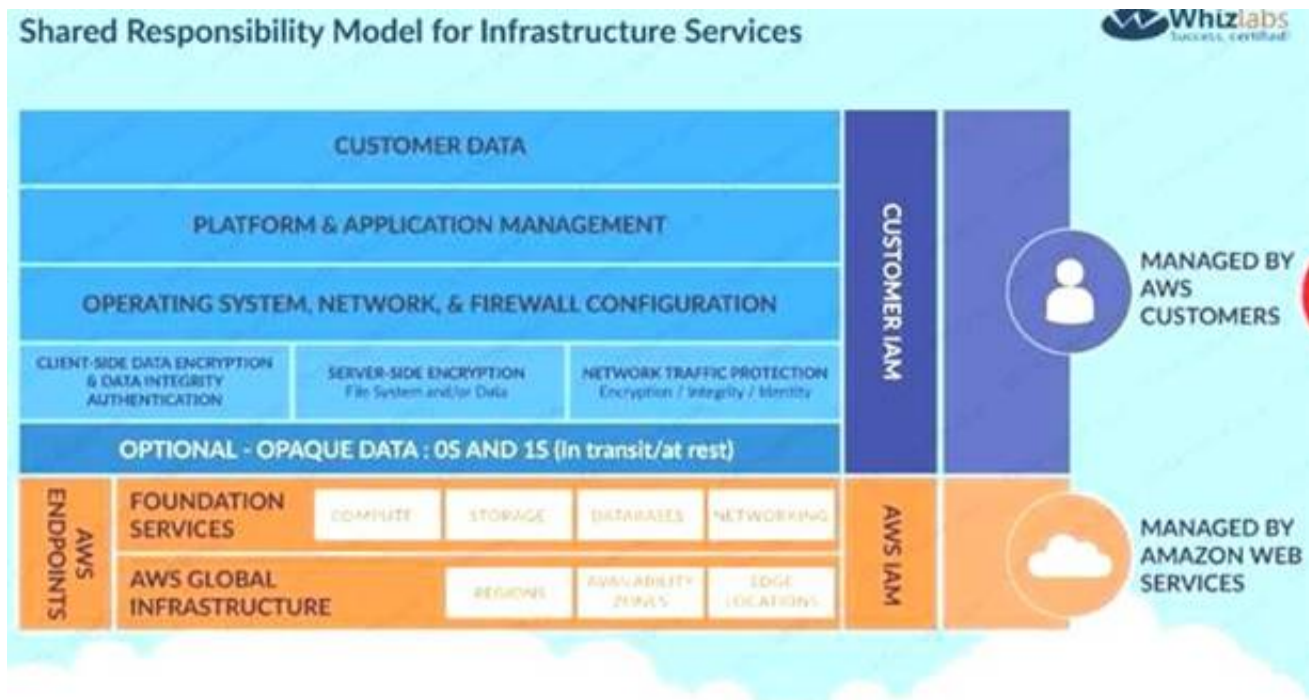Please select:

A. Management of the Edge locations
B. Encryption of data at rest
C. Protection of data in transit
D. Decommissioning of old storage devices

Answer: BC

Explanation:
Below is the snapshot of the Shared Responsibility Model

For more information on AWS Security best practises, please refer to below URL
.awsstatic corn/whitepapers/Security/AWS Practices.
The correct answers are: Encryption of data at rest Protection of data in transit Submit your Feedback/Queries to our Experts

NEW QUESTION 59
Your application currently use AWS Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How wou you manage the access effectively?
Please select:

A. Create different cognito endpoints, one for the readers and the other for the contributors.
B. Create different cognito groups, one for the readers and the other for the contributors.
C. You need to manage this within the application itself
D. This needs to be managed via Web security tokens

Answer: B

Explanation:
The AWS Documentation mentions the following
You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app.
Option A is incorrect since you need to create cognito groups and not endpoints
Options C and D are incorrect since these would be overheads when you can use AWS Cognito For more information on AWS Cognito user groups please refer to the below Link: https://docs.aws.amazon.com/coenito/latest/developersuide/cognito-user-pools-user-groups.htmll The correct answer is: Create different cognito groups, one for the readers and the other for the contributors. Submit your Feedback/Queries to our Experts

NEW QUESTION 62
A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that have occurred on AWS. How can the company meet the auditor's requirements without comprising security in the AWS environment? Choose the correct answer from the options below
Please select:

A. Create a role that has the required permissions for the auditor.
B. Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
C. The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to th^ third-party auditor.
D. Enable CloudTrail logging and create an 1AM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.

Answer: D

Explanation:
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.
Option A and C are incorrect since Cloudtrail needs to be used as part of the solution Option B is incorrect since the auditor needs to have access to Cloudtrail For more information on cloudtrail, please visit the below URL: https://aws.amazon.com/cloudtraiL
The correct answer is: Enable CloudTrail logging and create an 1AM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs. Submit your Feedback/Queries to our Experts

NEW QUESTION 65
An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below
Please select:

A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.<
B. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance

call.
C. Modify the 1AM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
D. Modify the 1AM policy on the user to require MFA before deleting EC2 instances

Answer: AB

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. Each tag consists of a key and an optional value, both of which you define
Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance.
For more information on tagging answer resources please refer to the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins_Tags.htmll
The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 66
A company has been using the AW5 KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below
Please select:

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

Answer: BC

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

NEW QUESTION 70
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 1AM user in the company account
B. Create an 1AM Role in the company account
C. Ensure the 1AM user has access for read-only to the S3 buckets
D. Ensure the 1AM 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 1AM role for each account that you want to share log files with.
For each of these 1AM roles, create an access policy that grants read-only access to the account you want to share the log files with.
Have an 1AM user in each account programmatically assume the appropriate role and retrieve the log files.
Options A and C are invalid because creating an 1AM user and then sharing the 1AM 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 1AM Role in the company account Ensure the 1AM Role has access for read-only to the S3 buckets
Submit your Feedback/Queries to our Experts

NEW QUESTION 74
Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner? Please select:

A. Grant public access for the bucket via the bucket policy
B. Use the aws:Referer key in the condition clause for the bucket policy
C. Use the aws:sites key in the condition clause for the bucket policy
D. Grant a role that can be assumed by the web site

Answer: B

Explanation:
An example of this is given intheAWS Documentatioi Restricting Access to a Specific HTTP Referrer
Suppose you have a website with domain name (www.example.com or example.com) with links to photos and videos stored in your S3 bucket examplebucket. By default, all the S3 resources are private, so only the AWS account that created the resources can access them. To allow read access to these objects from your website, you can add a bucket policy that allows s3:GetObject permission with a condition, using the aws:referer key, that the get request must originate from specific webpages. The following policy specifies the StringLike condition with the aws:Referer condition key.

```
{
  "Version":"2012-10-17",
  "Id":"http referer policy example",
  "Statement":[
    {
      "Sid":"Allow get requests originating from www.example.com and example.com.",
      "Effect":"Allow",
      "Principal":"*",
      "Action":"s3:GetObject",
      "Resource":"arn:aws:s3:::examplebucket/*",
      "Condition":{
        "StringLike":{"aws:Referer":["http://www.example.com/*","http://example.com/*"]}
      }
    }
  ]
}
```

Option A is invalid because giving public access is not a secure way to provide access Option C is invalid because aws:sites is not a valid condition key Option D is invalid because 1AM roles will not be assigned to web sites
For more information on example bucket policies please visit the below Link:
1 https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
The correct answer is: Use the aws:Referer key in the condition clause for the bucket policy Submit your Feedback/Queries to our Experts

NEW QUESTION 78
A company has a set of EC2 instances hosted in AWS. These instances have EBS volumes for storing critical information. There is a business continuity requirement and in order to boost the agility of the business and to ensure data durability which of the following options are not required.
Please select:

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

Answer: CD

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

NEW QUESTION 83
The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned 1AM policy statements allows the user to have access to the AWS usage report page?
Please select:

A. "Effect": "Allow". "Action": ["Describe"], "Resource": "Billing"

B. "Effect": "Allow", "Action": ["AccountUsage], "Resource": "*"
C. "Effect': "Allow", "Action": ["aws-portal:ViewUsage"," aws-portal:ViewBilling"], "Resource": "*"
D. "Effect": "Allow", "Action": ["aws-portal: ViewBilling"], "Resource": "*"

Answer: C

Explanation:
the aws documentation, below is the access required for a user to access the Usage reports page and as per this, Option C is the right answer.

Example 2: Allow IAM users to access the Reports console page

To allow an IAM user to access the **Reports** console page and to view the usage reports that contain account activity information. you would use a policy similar to this example policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewUsage",
                "aws-portal:ViewBilling"
            },
            "Resource": "*"
        }
    ]
}
```

NEW QUESTION 88
Your company looks at the gaming domain and hosts several Ec2 Instances as game servers. The servers each experience user loads in the thousands. There is a concern of DDos attacks on the EC2 Instances which could cause a huge revenue loss to the company. Which of the following can help mitigate this security concern and also ensure minimum downtime for the servers.
Please select:

A. Use VPC Flow logs to monitor the VPC and then implement NACL's to mitigate attacks
B. Use AWS Shield Advanced to protect the EC2 Instances
C. Use AWS Inspector to protect the EC2 Instances
D. Use AWS Trusted Advisor to protect the EC2 Instances

Answer: B

Explanation:
Below is an excerpt from the AWS Documentation on some of the use cases for AWS Shield

Example AWS Shield Advanced Use Cases

You can use Shield Advanced to protect your resources in many types of scenarios. However, in some cases you should use other services or combine other services with Shield Advanced to offer the best protection. Following are examples of how to use Shield Advanced or other AWS services to help protect your resources.

Goal	Suggested services	Related service documentation
Protect a web application and RESTful APIs against a DDoS attack	Shield Advanced protecting an Amazon CloudFront distribution and an Application Load Balancer	Amazon Elastic Load Balancing Documentation, Amazon CloudFront Documentation
Protect a TCP-based application against a DDoS attack	Shield Advanced protecting a Network Load Balancer attached to an Elastic IP address	Amazon Elastic Load Balancing Documentation
Protect a UDP-based game server against a DDoS attack	Shield Advanced protecting an Amazon EC2 instance attached to an Elastic IP address	Amazon Elastic Compute Cloud Documentation

NEW QUESTION 93
An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?
Please select:

A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
B. Create an 1AM user within the enterprise account assign a user policy to the 1AM user that allows only the actions required by the SaaS applicatio
C. Create a new access and secret key for the user and provide these credentials to the SaaS provider.
D. Create an 1AM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
E. Create an 1AM role for EC2 instances, assign it a policy that allows only the actions required tor the Saas application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

Answer: C

Explanation:
The below diagram from an AWS blog shows how access is given to other accounts for the services in your own account

Options A and B are invalid because you should not user 1AM users or 1AM Access keys Options D is invalid because you need to create a role for cross account access

For more information on Allowing access to external accounts, please visit the below URL:

|https://aws.amazon.com/blogs/apn/how-to-best-architect-your-aws-marketplace-saassubscription- across-multiple-aws-accounts;

The correct answer is: Create an 1AM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.

Submit your Feedback/Queries to our Experts

NEW QUESTION 96
Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.
Please select:
A.

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

B.

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

C.

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

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

A.

Answer: A

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

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

Submit your Feedback/Queries to our Expert

NEW QUESTION 97
You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?
Please select:

A. Add an AWS managed policy for the user
B. Add a service policy for the user
C. Add an 1AM role for the user
D. Add an inline policy for the user

Answer: D

Explanation:

Options A and B are incorrect since you need to add an inline policy just for the user Option C is invalid because you don't assign an 1AM role to a user
The AWS Documentation mentions the following
An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.
For more information on 1AM Access and Inline policies, just browse to the below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/access
The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

NEW QUESTION 99
Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?
Please select:

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

Answer: A

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

NEW QUESTION 101
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-Security-Specialty Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-Certified-Security-Specialty Product From:

https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/

Money Back Guarantee

AWS-Certified-Security-Specialty Practice Exam Features:

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

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

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

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