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
You are hosting a web site via website hosting on an S3 bucket - http://demo.s3-website-us-east-l .amazonaws.com. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages , they are getting a blocked Javascript error. How can you rectify this?
Please select:

A. Enable CORS for the bucket
B. Enable versioning for the bucket
C. Enable MFA for the bucket
D. Enable CRR for the bucket

Answer: A

Explanation:
Your answer is incorrect Answer-A
Such a scenario is also given in the AWS Documentation Cross-Origin Resource Sharing:
Use-case Scenarios
The following are example scenarios for using CORS:
• Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint http://website.s3-website-us-east-1 .amazonaws.com. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1 .amazonaws.com.
• Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.
Option Bis invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects
Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects
For more information on Cross Origin Resource sharing, please visit the following URL
• ittps://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html
The correct answer is: Enable CORS for the bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 3
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 4
You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks. Which of the following service can help in such a scenario
Please select:

A. AWS Trusted Advisor
B. AWS WAF
C. AWS Inspector
D. AWS Config

Answer: B

Explanation:
The AWS Documentation mentions the following
AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common
web explogts like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect. Option A is invalid because this will only give advise on how you can better the security in your AWS account but not protect against threats mentioned in the question.
Option C is invalid because this can be used to scan EC2 Instances for vulnerabilities but not protect against threats mentioned in the question.
Option D is invalid because this can be used to check config changes but not protect against threats mentioned in the quest
For more information on AWS WAF, please visit the following URL: https://aws.amazon.com/waf/details;
The correct answer is: AWS WAF
Submit your Feedback/Queries to our Experts

NEW QUESTION 5
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 6
You are deivising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

```
{ "ID": "Policy1502987489630",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1502987487640",
"Action": [
"s3:GetObject",
"s3:GetObjectVersion"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::appbucket",
"Principal": "*"
}
]
}
```

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error
Please select:

A. Change the 1AM permissions by applying PutBucketPolicy permissions.
B. Verify that the policy has the same name as the bucket nam
C. If no
D. make it the same.
E. Change the Resource section to "arn:aws:s3:::appbucket/*'.
F. Create the bucket "appbucket" and then apply the polic

Answer: C

Explanation:
When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket
Option A is invalid because the right permissions are already provided as per the question requirement
Option B is invalid because it is not necessary that the policy has the same name as the bucket Option D is invalid because this should be the default flow for applying the policy
For more information on bucket policies please visit the below URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.htmll
The correct answer is: Change the Resource section to "arn:aws:s3:::appbucket/" Submit your Feedback/Queries to our Experts

NEW QUESTION 7
You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?
Please select:

A. Enable AWS Guard Duty for the Instance
B. Use AWS Trusted Advisor
C. Use AWS inspector
D. UseAWSMacie

Answer: C

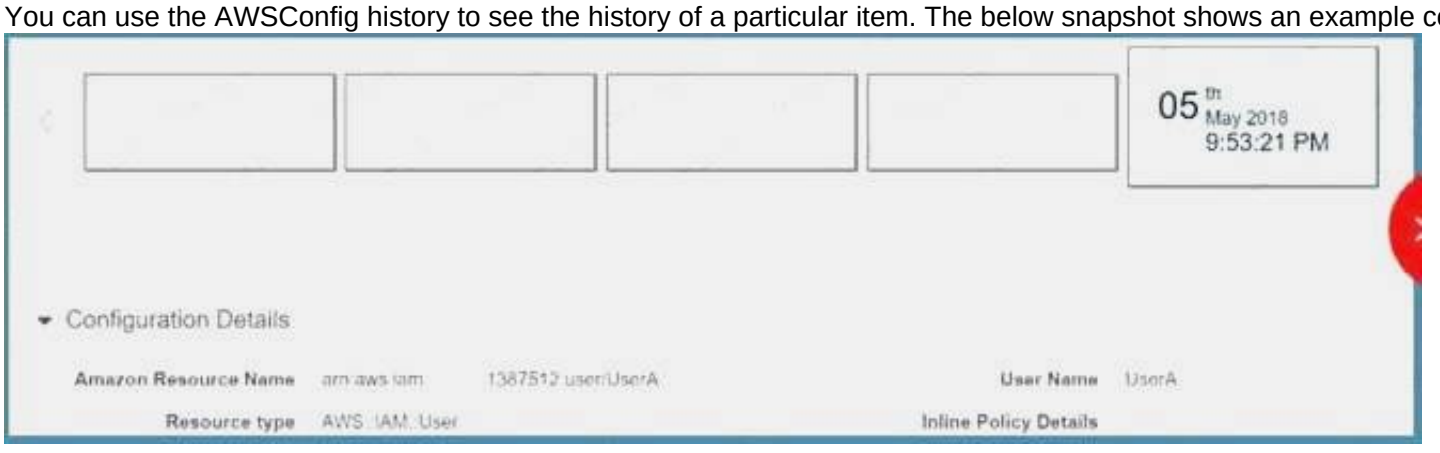
Explanation:
The AWS Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security
Center for Internet security (CIS) Benchmarks
The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed nere.
Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities
Options B and D are invalid because these services cannot give a list of vulnerabilities For more information on the guidelines, please visit the below URL:
* https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html The correct answer is: Use AWS Inspector
Submit your Feedback/Queries to our Experts

NEW QUESTION 8
A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee's 1AM permissions changed as part of the incident.
What steps should the team document in the plan? Please select:

A. Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
B. Use Made to examine the employee's 1AM permissions prior to the incident and compare them to the employee's A current 1AM permissions.
C. Use CloudTrail to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.
D. Use Trusted Advisor to examine the employee's 1AM permissions prior to the incident and compare them to the employee's current 1AM permissions.

Answer: A

Explanation:
You can use the AWSConfig history to see the history of a particular item. The below snapshot shows an example configuration for a user in AWS Config



Option B,C and D are all invalid because these services cannot be used to see the history of a particular configuration item. This can only be accomplished by AWS Config.
For more information on tracking changes in AWS Config, please visit the below URL:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackineChanees.htmll The correct answer is: Use AWS Config to examine the employee's 1AM permissions prior to the incident and compare them the employee's current 1AM permissions.
Submit your Feedback/Queries to our Experts

NEW QUESTION 9
Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account.
Please select:

A. Delete the AWS keys for the root account
B. Create 1AM Groups
C. Create 1AM Roles
D. Restrict access using 1AM policies

Answer: A

Explanation:
The first level or measure that should be taken is to delete the keys for the 1AM root user
When you log into your account and go to your Security Access dashboard, this is the first step that can be seen

Option B and C are wrong because creation of 1AM groups and roles will not change the impact of leakage of AWS root access keys
Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL: https://docs.aws.amazon.com/eeneral/latest/gr/aws-access-keys-best-practices.html
The correct answer is: Delete the AWS keys for the root account Submit your Feedback/Queries to our Experts

NEW QUESTION 10
Which of the following is not a best practice for carrying out a security audit? Please select:

A. Conduct an audit on a yearly basis
B. Conduct an audit if application instances have been added to your account
C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
D. Whenever there are changes in your organization

Answer: A

Explanation:
A year's time is generally too long a gap for conducting security audits The AWS Documentation mentions the following
You should audit your security configuration in the following situations: On a periodic basis.
If there are changes in your organization, such as people leaving.
If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need.
If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWor stacks, AWS CloudFormation templates, etc.
If you ever suspect that an unauthorized person might have accessed your account.
Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits For more information on Security Audit guideline, please visit the below URL: https://docs.aws.amazon.com/eeneral/latest/gr/aws-security-audit-euide.html
The correct answer is: Conduct an audit on a yearly basis Submit your Feedback/Queries to our Experts

NEW QUESTION 10
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

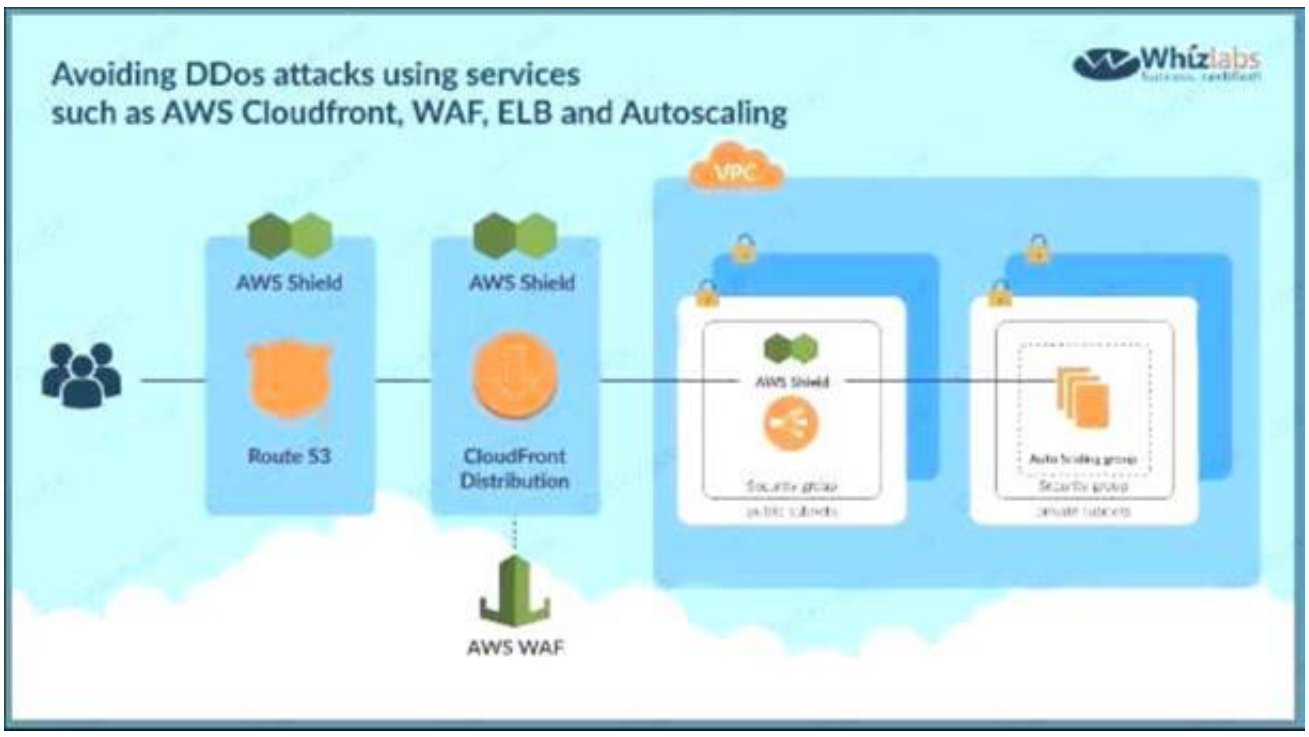
Explanation:
After the VPC peering connection is established, you need to ensure that the route tables are modified to ensure traffic can between the VPCs
Option A ,B and C are invalid because allowing access the Internet gateway and usage of public subnets can help for Inter, access, but not for VPC 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 15
A company is deploying a new web application on AWS. Based on their other web applications, they
anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect their application? Select 2 answers from the options given below.
Please select:

A. Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.
B. Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
C. Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
D. Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
E. Enable GuardDuty to block malicious traffic from reaching the application

Answer: BD

Explanation:
The below diagram from AWS shows the best case scenario for avoiding DDos attacks using services such as AWS Cloudfro WAF, ELB and Autoscaling



Option A is invalid because by default security groups don't allow access Option C is invalid because AWS Inspector cannot be used to examine traffic
Option E is invalid because this can be used for attacks on EC2 Instances but not against DDos attacks on the entire application For more information on DDos mitigation from AWS, please visit the below URL:
https://aws.amazon.com/answers/networking/aws-ddos-attack-mitieationi
The correct answers are: Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic., Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
Submit your Feedback/Queries to our Experts

NEW QUESTION 20
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 21
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 26
Your company makes use of S3 buckets for storing dat

A. There is a company policy that all services should have logging enable

B. How can you ensure thatlogging is always enabled for created S3 buckets in the AWS Account? Please select:
C. Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
D. Use AWS Config Rules to check whether logging is enabled for buckets
E. Use AWS Cloudwatch metrics to check whether logging is enabled for buckets
F. 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 30
An application running on EC2 instances in a VPC must access sensitive data in the data center. The access must be encrypted in transit and have consistent low latency. Which hybrid architecture will meet these requirements?
Please select:
A. Expose the data with a public HTTPS endpoint.
B. A VPN between the VPC and the data center over a Direct Connect connection
C. A VPN between the VPC and the data center.
D. A Direct Connect connection between the VPC and data center

Answer: B

Explanation:
Since this is required over a consistency low latency connection, you should use Direct Connect. For encryption, you can make use of a VPN
Option A is invalid because exposing an HTTPS endpoint will not help all traffic to flow between a VPC and the data center.
Option C is invalid because low latency is a key requirement Option D is invalid because only Direct Connect will not suffice
For more information on the connection options please see the below Link: https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharint
The correct answer is: A VPN between the VPC and the data center over a Direct Connect connection Submit your Feedback/Queries to our Experts

NEW QUESTION 33
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 37
A company wishes to enable Single Sign On (SSO) so its employees can login to the management console using their corporate directory identity. Which steps below are required as part of the process? Select 2 answers from the options given below.
Please select:

A. Create a Direct Connect connection between on-premise network and AW
B. Use an AD connector for connecting AWS with on-premise active directory.
C. Create 1AM policies that can be mapped to group memberships in the corporate directory.
D. Create a Lambda function to assign 1AM roles to the temporary security tokens provided to the users.
E. Create 1AM users that can be mapped to the employees' corporate identities
F. Create an 1AM role that establishes a trust relationship between 1AM and the corporate directory identity provider (IdP)

Answer: AE

Explanation:
Create a Direct Connect connection so that corporate users can access the AWS account
Option B is incorrect because 1AM policies are not directly mapped to group memberships in the corporate directory. It is 1AM roles which are mapped.
Option C is incorrect because Lambda functions is an incorrect option to assign roles.
Option D is incorrect because 1AM users are not directly mapped to employees' corporate identities. For more information on Direct Connect, please refer to below

URL:
' https://aws.amazon.com/directconnect/
From the AWS Documentation, for federated access, you also need to ensure the right policy permissions are in place
Configure permissions in AWS for your federated users
The next step is to create an 1AM role that establishes a trust relationship between 1AM and your organization's IdP that identifies your IdP as a principal (trusted entity) for purposes of federation. The role also defines what users authenticated your organization's IdP are allowed to do in AWS. You can use the 1AM console to create this role. When you create the trust policy that indicates who can assume the role, you specify the SAML provider that you created earlier in 1AM along with one or more SAML attributes that a user must match to be allowed to assume the role. For example, you can
specify that only users whose SAML eduPersonOrgDN value is ExampleOrg are allowed to sign in. The role wizard automatically adds a condition to test the saml:aud attribute to make sure that the role is assumed only for sign-in to the AWS Management Console. The trust policy for the role might look like this:

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {"Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/ExampleOrgSSOProvider"},
  "Action": "sts:AssumeRoleWithSAML",
  "Condition": {"StringEquals": {
   "saml:edupersonorgdn": "ExampleOrg",
   "saml:aud": "https://signin.aws.amazon.com/saml"
  }}
 }]
}
```

For more information on SAML federation, please refer to below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enabli Note:
What directories can I use with AWS SSO?
You can connect AWS SSO to Microsoft Active Directory, running either on-premises or in the AWS Cloud. AWS SSO supports AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, and AD Connector. AWS SSO does not support Simple AD. See AWS Directory Service Getting Started to learn more.
To connect to your on-premises directory with AD Connector, you need the following: VPC
Set up a VPC with the following:
• At least two subnets. Each of the subnets must be in a different Availability Zone.
• The VPC must be connected to your on-premises network through a virtual private network (VPN)
connection or AWS Direct Connect.
• The VPC must have default hardware tenancy.
• https://aws.amazon.com/single-sign-on/
• https://aws.amazon.com/single-sign-on/faqs/
• https://aws.amazon.com/bloj using-corporate-credentials/
• https://docs.aws.amazon.com/directoryservice/latest/admin-
The correct answers are: Create a Direct Connect connection between on-premise network and AWS. Use an AD connector connecting AWS with on-premise active directory.. Create an 1AM role that establishes a trust relationship between 1AM and corporate directory identity provider (IdP)
Submit your Feedback/Queries to our Experts

NEW QUESTION 39
A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below
Please select:

A. AWS VPN
B. AWS VPC Peering
C. AWS NAT gateways
D. AWS Direct Connect

Answer: AD

Explanation:
The AWS Document mention the following which supports the requirement

VPN Connections

You can connect your Amazon VPC to remote networks by using a VPN connection. The following are some of the connectivity options available to you.

VPN connectivity option	Description
AWS managed VPN	You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a *virtual private gateway* provides two VPN endpoints (tunnels) for automatic failover. You configure your *customer gateway* on the remote side of the VPN connection. For more information, see AWS Managed VPN Connections, and the Amazon VPC Network Administrator Guide.
AWS VPN CloudHub	If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks. For more information, see Providing Secure Communication Between Sites Using VPN CloudHub.
Third party software VPN appliance	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third party software VPN appliance. AWS does not provide or maintain third party software VPN appliances; however, you can choose from a range of products provided by partners and open source communities. Find third party software VPN appliances on the AWS Marketplace.

You can also use AWS Direct Connect to create a dedicated private connection from a remote network to your VPC. You can combine this connection with an AWS managed VPN connection to create an IPsec-encrypted connection. For more information, see What is AWS Direct Connect? in the *AWS Direct Connect User Guide*. For more information about the different VPC and VPN connectivity options, see the Amazon Virtual Private Cloud Connectivity Options whitepaper.

Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the AWS Cloud.
Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet For more information on VPN Connections, please visit the following url https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html
The correct answers are: AWS VPN, AWS Direct Connect Submit your Feedback/Queries to our Experts

NEW QUESTION 44
How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance. How can this be achieved?
Please select:

A. Change the existing DHCP options set
B. Create a new DHCP options set and replace the existing one.
C. Change the route table for the VPC
D. Change the subnet configuration to allow DNS requests from the new DNS Server

Answer: B

Explanation:
In order to use your own DNS server, you need to ensure that you create a new custom DHCP options set with the IP of th custom DNS server. You cannot modify the existing set, so you need to create a new one.
Option A is invalid because you cannot make changes to an existing DHCP options Set.
Option C is invalid because this can only be used to work with Routes and not with a custom DNS solution.
Option D is invalid because this needs to be done at the VPC level and not at the Subnet level For more information on DHCP options set, please visit the following url https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC DHCP Options.html
The correct answer is: Create a new DHCP options set and replace the existing one. Submit your Feedback/Queries to our Experts

NEW QUESTION 47
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 52
You have an EBS volume attached to an EC2 Instance which uses KMS for Encryption. Someone has now gone ahead and deleted the Customer Key which was used for the EBS encryption. What should be done to ensure the data can be decrypted.
Please select:

A. Create a new Customer Key using KMS and attach it to the existing volume
B. You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable.
C. Request AWS Support to recover the key
D. Use AWS Config to recover the key

Answer: B

Explanation:
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.
https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html
A is incorrect because Creating a new CMK and attaching it to the exiting volume will not allow the data to be decrypted, you cannot attach customer master keys after the volume is encrypted
Option C and D are invalid because once the key has been deleted, you cannot recover it For more information on EBS Encryption with KMS, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html
The correct answer is: You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable. Submit your Feedback/Queries to our Experts

NEW QUESTION 57
You work as an administrator for a company. The company hosts a number of resources using AWS. There is an incident of a suspicious API activity which occurred 11 days ago. The Security Admin has asked to get the API activity from that point in time. How can this be achieved?
Please select:

A. Search the Cloud Watch logs to find for the suspicious activity which occurred 11 days ago
B. Search the Cloudtrail event history on the API events which occurred 11 days ago.
C. Search the Cloud Watch metrics to find for the suspicious activity which occurred 11 days ago

D. Use AWS Config to get the API calls which were made 11 days ag

Answer: B

Explanation:
The Cloud Trail event history allows to view events which are recorded for 90 days. So one can use a metric filter to gather the API calls from 11 days ago.
Option A and C is invalid because Cloudwatch is used for logging and not for monitoring API activity Option D is invalid because AWSConfig is a configuration service and not for monitoring API activity For more information on AWS Cloudtrail, please visit the following URL:
https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/how-cloudtrail-works.html
Note:
In this question we assume that the customer has enabled cloud trail service.
AWS CloudTrail is enabled by default for ALL CUSTOMERS and will provide visibility into the past seven days of account activity without the need for you to configure a trail in the service to get started. So for an activity that happened 11 days ago to be stored in the cloud trail we need to configure the trail manually to ensure that it is stored in the events history.
• https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-awscustomers/ The correct answer is: Search the Cloudtrail event history on the API events which occurred 11 days ago.

NEW QUESTION 59
You need to ensure that the cloudtrail logs which are being delivered in your AWS account is encrypted. How can this be achieved in the easiest way possible? Please select:

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

Answer: A

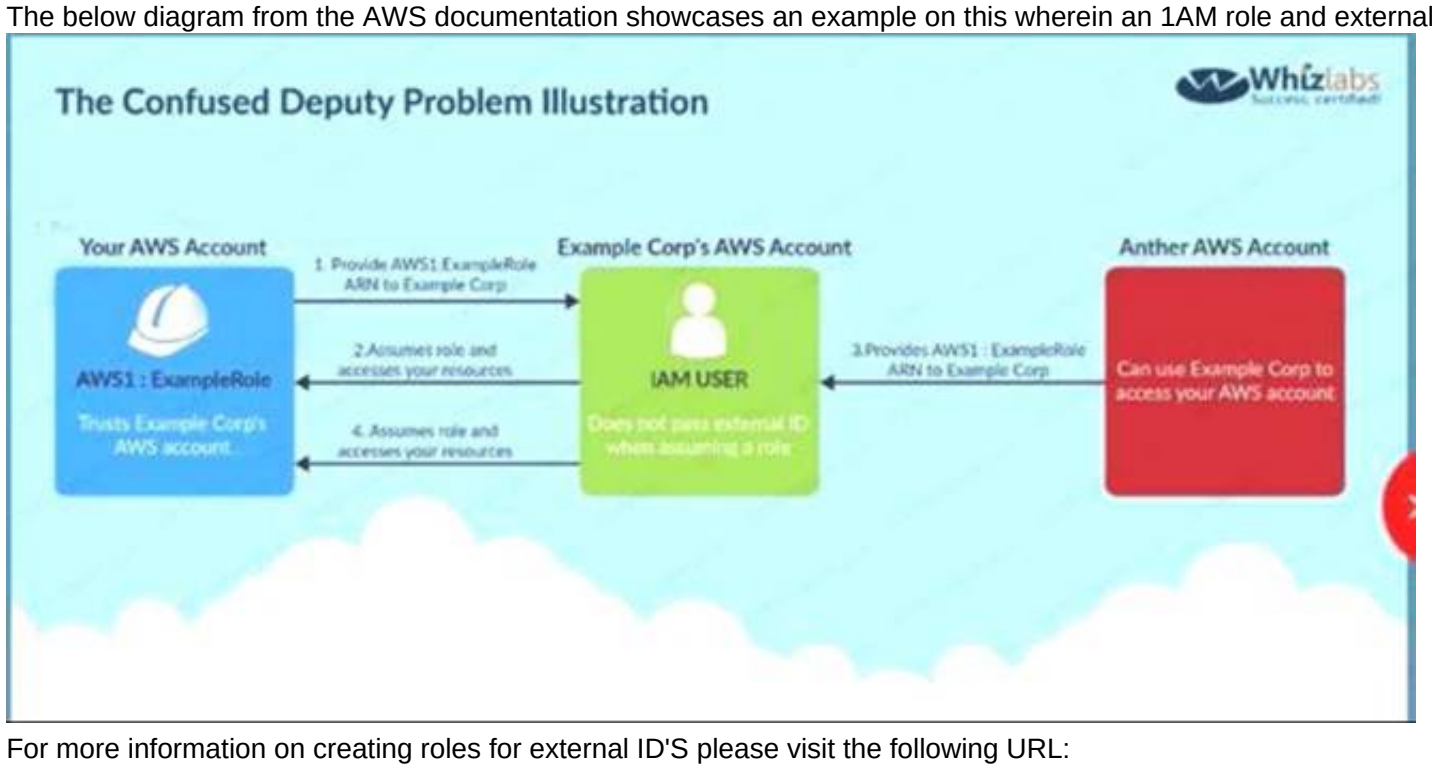
Explanation:
The AWS Documentation mentions the following
By default the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side
encryption with Amazon S3-managed encryption keys (SSE-S3)
Option B,C and D are all invalid because by default all logs are encrypted when they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

NEW QUESTION 62
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 1AM role is created which can be assumed by the partner account.
B. Ensure an 1AM 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 1AM 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 1AM role and external ID is us> access an AWS account resources



For more information on creating roles for external ID'S please visit the following URL:
The correct answers are: Ensure an 1AM 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

NEW QUESTION 67

Your company has a requirement to work with a DynamoDB table. There is a security mandate that all data should be encrypted at rest. What is the easiest way to accomplish this for DynamoDB. Please select:

A. Use the AWS SDK to encrypt the data before sending it to the DynamoDB table
B. Encrypt the DynamoDB table using KMS during its creation
C. Encrypt the table using AWS KMS after it is created
D. Use S3 buckets to encrypt the data before sending it to DynamoDB

Answer: B

Explanation:
The most easiest option is to enable encryption when the DynamoDB table is created. The AWS Documentation mentions the following
Amazon DynamoDB offers fully managed encryption at rest. DynamoDB encryption at rest provides enhanced security by encrypting your data at rest using an AWS Key Management Service (AWS KMS) managed encryption key for DynamoDB. This functionality eliminates the operational burden and complexity involved in protecting sensitive data.
Option A is partially correct, you can use the AWS SDK to encrypt the data, but the easier option would be to encrypt the table before hand.
Option C is invalid because you cannot encrypt the table after it is created
Option D is invalid because encryption for S3 buckets is for the objects in S3 only.
For more information on securing data at rest for DynamoDB please refer to below URL:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.htmll The correct answer is: Encrypt the DynamoDB table using KMS during its creation Submit your Feedback/Queries to our Experts

NEW QUESTION 71
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

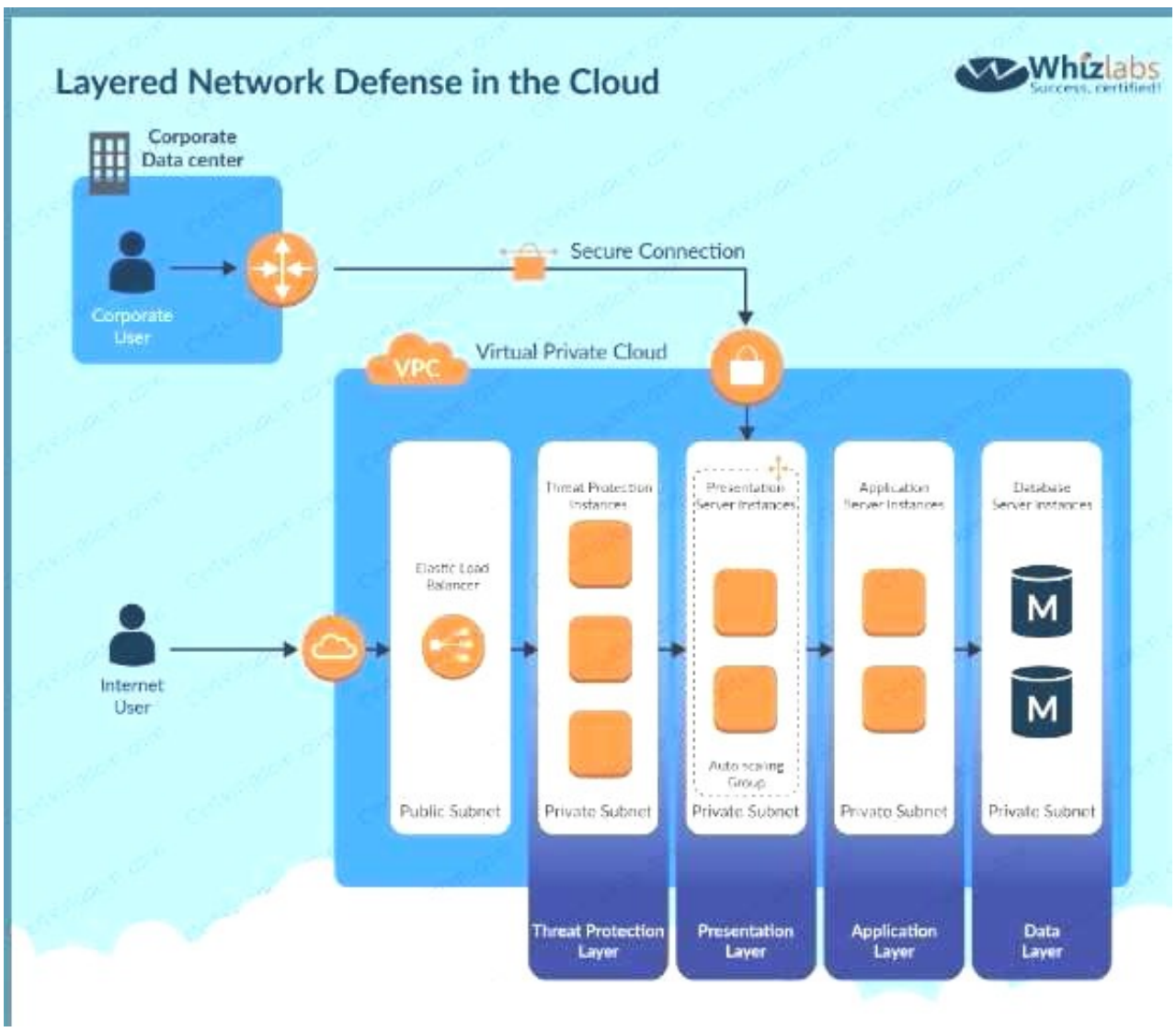
Explanation:
Some of the important aspects in such a situation are
1) First isolate the instance so that no further security harm can occur on other AWS resources
2) Take a snapshot of the EBS volume for further investigation. This is incase if you need to shutdown the initial instance and do a separate 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 74
Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below
Please select:

A. Use a host based intrusion detection system
B. Use a third party firewall installed on a central EC2 instance
C. Use VPC Flow logs
D. Use Network Access control lists logging

Answer: AB

Explanation:
If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the AWS Security best practices



Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on AWS Security best practices, please refer to below URL:
The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2
Submit your Feedback/Queries to our Experts

NEW QUESTION 78
Your company use AWS KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities. What can be done during the deletion process to verify that the key is no longer being used.
Please select:

A. Use CloudTrail to see if any KMS API request has been issued against existing keys
B. Use Key policies to see the access level for the keys
C. Rotate the keys once before deletion to see if other services are using the keys
D. Change the 1AM policy for the keys to see if other services are using the keys

Answer: A

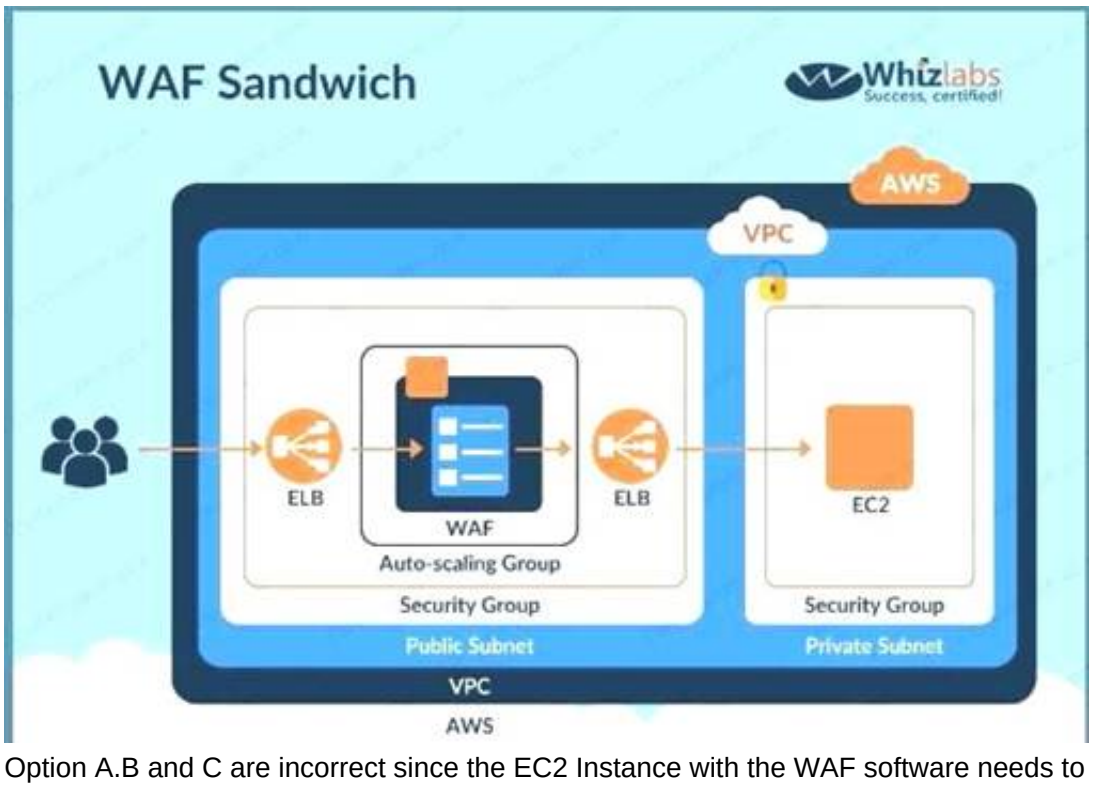
Explanation:
The AWS lentation mentions the following
You can use a combination of AWS CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it
Options B and D are incorrect because Key policies nor 1AM policies can be used to check if the keys are being used.
Option C is incorrect since rotation will not help you check if the keys are being used. For more information on deleting keys, please refer to below URL:
https://docs.aws.amazon.com/kms/latest/developereuide/deletine-keys-creatine-cloudwatchalarm. html
The correct answer is: Use CloudTrail to see if any KMS API request has been issued against existing keys Submit your Feedback/Queries to our Experts

NEW QUESTION 83
DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich." Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below
Please select:

A. The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the internet.
B. The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
C. The EC2 instance running your WAF software is placed between your public subnets and your private subnets.
D. he EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

Answer: D

Explanation:
The below diagram shows how a WAF sandwich is created. Its the concept of placing the Ec2 instance which hosts the WAF software in between 2 elastic load balancers.



Option A.B and C are incorrect since the EC2 Instance with the WAF software needs to be placed in an Autoscaling Group For more information on a WAF sandwich please refer to the below Link: https://www.cloudaxis.eom/2016/11/2l/waf-sandwich/l
The correct answer is: The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.
Submit your Feedback/Queries to our Experts

NEW QUESTION 88
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 CIoudTrail 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 93
An auditor needs access to logs that record all API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below
Please select:

A. Configure the CloudTrail service in each AWS account, and have the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary 1AM account that can assume a read-only role in the secondary AWS accounts.
B. Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary account
C. Then grant the auditor access to the S3 bucket that receives theCloudTrail log files.
D. Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.
E. Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and erant the auditor access to that single bucket in the orimarvaccoun

Answer: D

Explanation:
Given the current requirements, assume the method of "least privilege" security design and only allow the auditor access to the minimum amount of AWS resources as possibli
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
only be granted access in one location
Option Option A is incorrect since the auditor should B is incorrect since consolidated billing is not a key requirement as part of the question
Option C is incorrect since there is not consolidated logging
For more information on Cloudtrail please refer to the below URL: https://aws.amazon.com/cloudtraiL
(

The correct answer is: Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bud in the primary account and grant the auditor access to that single bucket in the primary account.
Submit your Feedback/Queries to our Experts

NEW QUESTION 96
You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets. Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below
Please select:

A. 1AM policies
B. Buckets ACL's
C. 1AM users
D. Bucket policies

Answer: BD

Explanation:
The AWS Security whitepaper gives the type of access control and to what level the control can be given

Type of Access Control	AWS Account-Level Control?	User-LevelControl?
IAM Policies	No	Yes
ACLs	Yes	No
Bucket Policies	Yes	Yes

Options A and C are incorrect since for external access to buckets, you need to use either Bucket policies or Bucket ACL's or more information on Security for storage services role please refer to the below URL:
https://d1.awsstatic.com/whitepapers/Security/Security Storage Services Whitepaper.pdf The correct answers are: Buckets ACL's, Bucket policies
Submit your Feedback/Queries to our Experts

NEW QUESTION 101
Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following
Whether any ports are left open other than admin ones like SSH and RDP
Whether any ports to the database server other than ones from the web server security group are
open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?
Please select:

A. AWS Config
B. AWS Trusted Advisor
C. AWS Inspector D.AWSGuardDuty

Answer: B

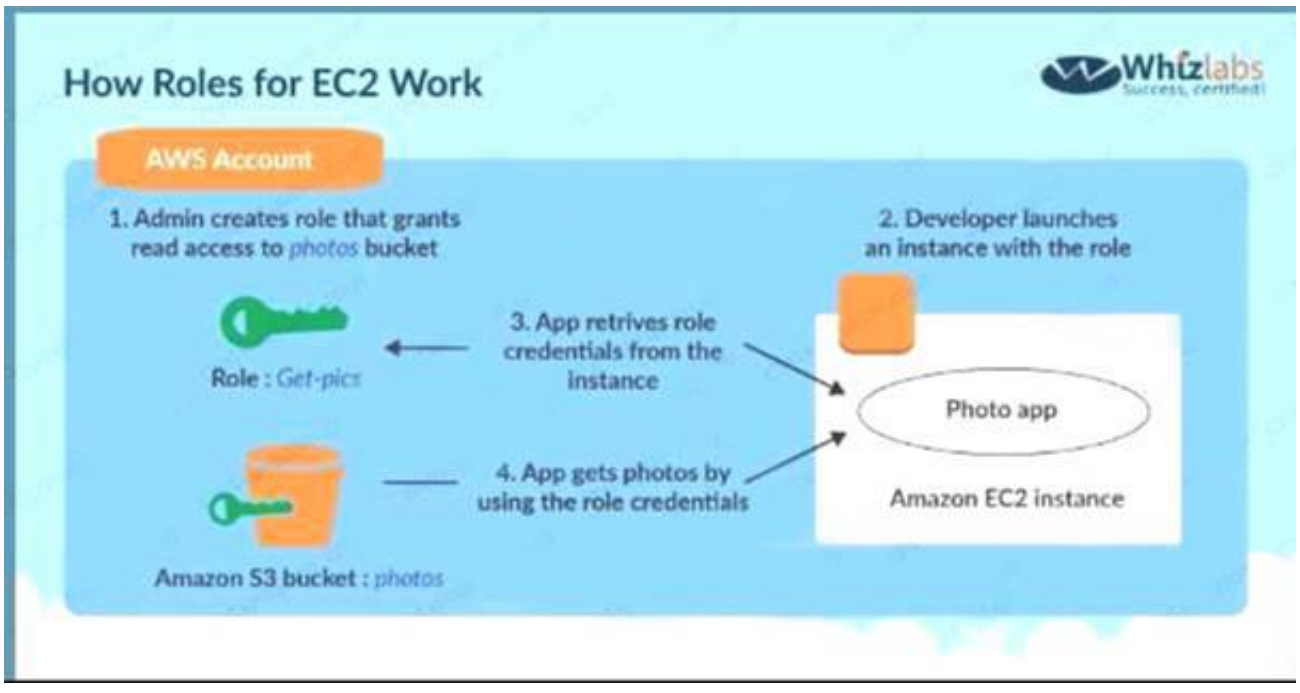
Explanation:
Trusted Advisor checks for compliance with the following security recommendations:
Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNQ.
Limited access to common database ports. This includes ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).
Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all o these checks on its dashboard
Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in th.
assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2
instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and
configuration data (telemetry), which it then passes to the Amazon Inspector service.
Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this)
question.
Options D is invalid because this service dont provide these details.
For more information on the Trusted Advisor, please visit the following URL https://aws.amazon.com/premiumsupport/trustedadvisor>
The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 105
An application is designed to run on an EC2 Instance. The applications needs to work with an S3 bucket. From a security perspective , what is the ideal way for the EC2 instance/ application to be configured?
Please select:

A. Use the AWS access keys ensuring that they are frequently rotated.
B. Assign an 1AM user to the application that has specific access to only that S3 bucket
C. Assign an 1AM Role and assign it to the EC2 Instance
D. Assign an 1AM group and assign it to the EC2 Instance

Answer: C

Explanation:
The below diagram from the AWS whitepaper shows the best security practicse of allocating a role that has access to the S3 bucket



Options A,B and D are invalid because using users, groups or access keys is an invalid security practise when giving access to resources from other AWS resources.
For more information on the Security Best practices, please visit the following URL: https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl
The correct answer is: Assign an 1AM Role and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 110
Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below
Please select:

A. AWS Cloudfront
B. AWS Lambda
C. AWS Application Load Balancer
D. AWS Classic Load Balancer

Answer: AC

Explanation:
The AWS documentation mentions the following on the Application Load Balancer
AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it car be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.
Options B and D are invalid because only Cloudfront and the Application Load Balancer services are supported by AWS WAF.
For more information on the web application firewall please refer to the below URL: https://aws.amazon.com/waf/faq;
The correct answers are: AWS Cloudfront AWS Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 114
A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion. What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below Please select:

A. Enable versioning on the S3 bucket
B. Enable data at rest for the objects in the bucket
C. Enable MFA Delete in the bucket policy
D. Enable data in transit for the objects in the bucket

Answer: AC

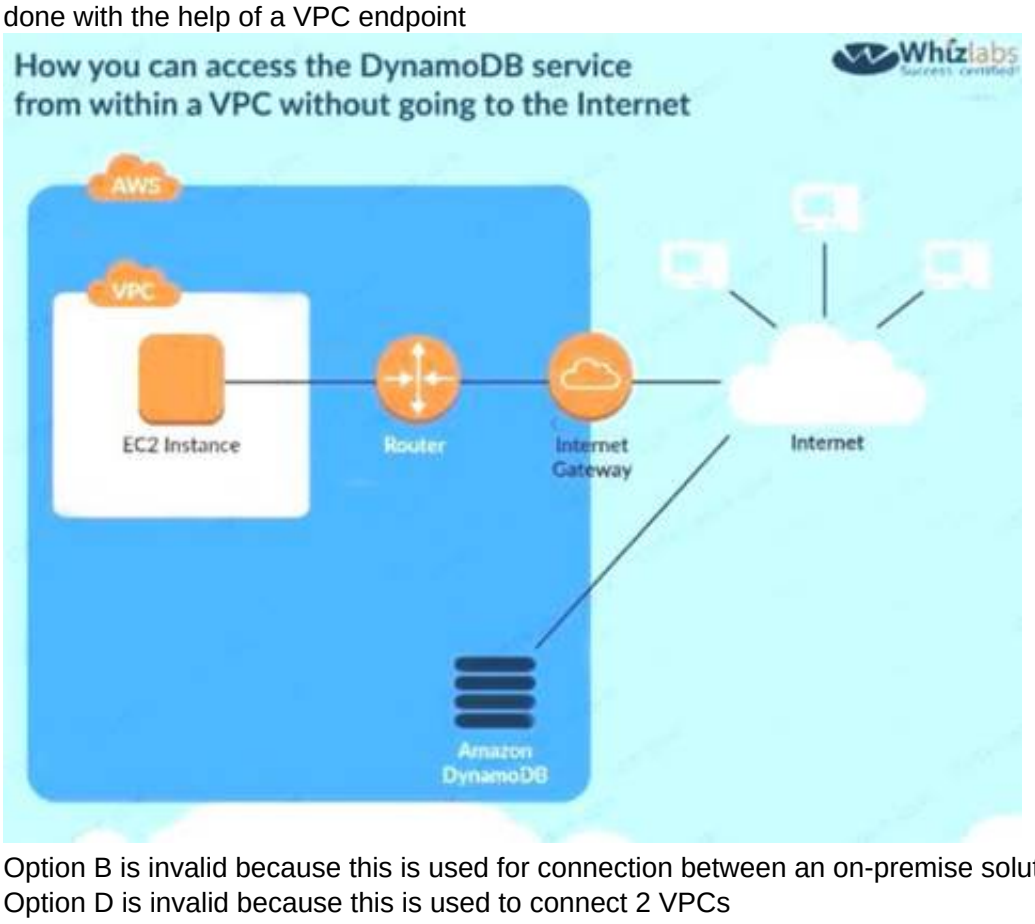
Explanation:
One of the AWS Security blogs mentions the followinj
Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request.
You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your AWS accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket. Option B is invalid because enabling encryption does not guarantee risk of data deletion.
Option D is invalid because this option does not guarantee risk of data deletion.
For more information on AWS S3 versioning and MFA please refer to the below URL: https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/

NEW QUESTION 115
There is a set of Ec2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?
Please select:

A. Use a VPC endpoint to the DynamoDB table
B. Use a VPN connection from the VPC
C. Use a VPC gateway from the VPC
D. Use a VPC Peering connection to the DynamoDB table

Answer: A

Explanation:
The following diagram from the AWS Documentation shows how you can access the DynamoDB service from within a V without going to the Internet This can be done with the help of a VPC endpoint



Option B is invalid because this is used for connection between an on-premise solution and AWS Option C is invalid because there is no such option
Option D is invalid because this is used to connect 2 VPCs
For more information on VPC endpointsfor DynamoDB, please visit the URL:
The correct answer is: Use a VPC endpoint to the DynamoDB table Submit your Feedback/Queries to our Experts

NEW QUESTION 119
You need to establish a secure backup and archiving solution for your company, using AWS. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which AWS service fulfills these requirements in the most cost-effective way?
Choose the correct answer
Please select:

A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.
C. Use Direct Connect to upload data to S3 and use 1AM policies to move the data into Glacier for long-term archiving.
D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

Answer: A

Explanation:
amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as
$0,004 per gigabyte per month, a significant savings compared to on-premises solutions.
With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARDJA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.
Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because 1AM policies cannot be used to move data to Glacier
Option D is invalid because lifecycle policies is not used to move data to Redshif For more information on S3 lifecycle policies, please visit the URL:
http://docs.aws.amazon.com/AmazonS3/latest/dev/obiect-lifecycle-mgmt.html
The correct answer is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.
Submit your Feedback/Queries to our Experts

NEW QUESTION 124
In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being recreated.
What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below
Please select:

A. Give only the necessary access to the Apache servers so that the developers can gain access to thelog files.
B. Give root access to your Apache servers to the developers.
C. Give read-only access to your developers to the Apache servers.
D. Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Answer: D

Explanation:
One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective.
The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3.
Options A,B and C are all invalid because you should not give access to the developers on the Apache se
For more information on S3, please refer to the below link https://aws.amazon.com/documentation/s3j
The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.
Submit vour Feedback/Queries to our Experts

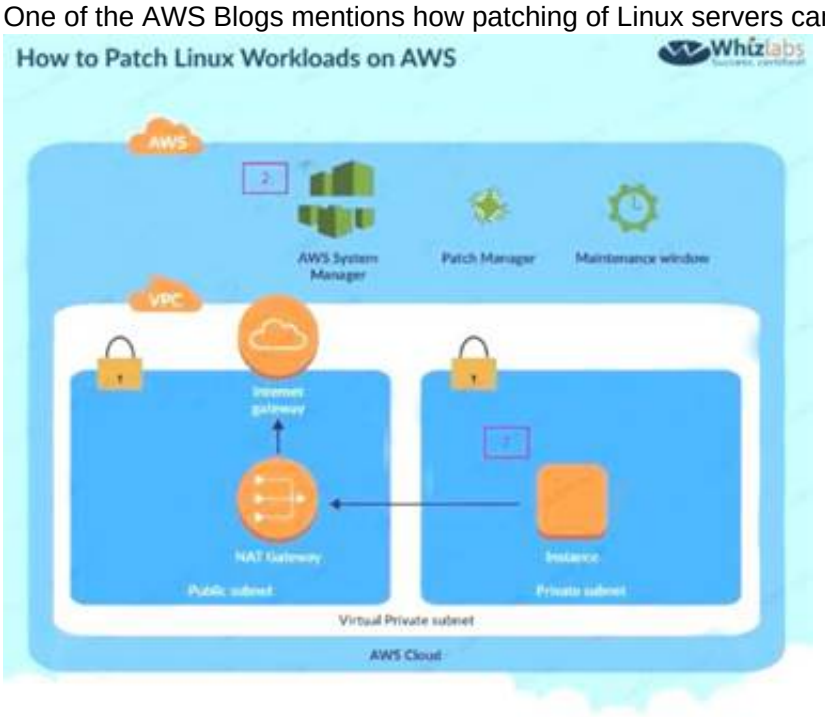
NEW QUESTION 125

You have a set of 100 EC2 Instances in an AWS account. You need to ensure that all of these instances are patched and kept to date. All of the instances are in a private subnet. How can you achieve this. Choose 2 answers from the options given below
Please select:

A. Ensure a NAT gateway is present to download the updates
B. Use the Systems Manager to patch the instances
C. Ensure an internet gateway is present to download the updates
D. Use the AWS inspector to patch the updates

Answer: AB

Explanation:
Option C is invalid because the instances need to remain in the private: Option D is invalid because AWS inspector can only detect the patches
One of the AWS Blogs mentions how patching of Linux servers can be accomplished. Below is the diagram representation of the architecture setup



For more information on patching Linux workloads in AWS, please refer to the Lin. https://aws.amazon.com/blogs/security/how-to-patch-linux-workloads-on-awsj
The correct answers are: Ensure a NAT gateway is present to download the updates. Use the Systems Manager to patch the instances
Submit your Feedback/Queries to our Experts

NEW QUESTION 127
Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?
Please select:

A. Use the application to rotate the keys in every 2 months via the SDK
B. Use a script to query the creation date of the key
C. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.
D. Delete the user associated with the keys after every 2 month
E. Then recreate the user again.
F. Delete the 1AM Role associated with the keys after every 2 month
G. Then recreate the 1AM Role again.

Answer: B

Explanation:
One can use the CLI command list-access-keys to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted.
The Returns list-access-keys CLI command returns information about the access key IDs associated with the specified 1AM user. If there are none, the action returns an empty list
Option A is incorrect because you might as use a script for such maintenance activities Option C is incorrect because you would not rotate the users themselves
Option D is incorrect because you don't use 1AM roles for such a purpose
For more information on the CLI command, please refer to the below Link: http://docs.aws.amazon.com/cli/latest/reference/iam/list-access-keys.htmll
The correct answer is: Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it. Submit your Feedback/Queries to our Experts

NEW QUESTION 131
.....

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