SCS-C01 Dumps

AWS Certified Security- Specialty

https://www.certleader.com/SCS-C01-dumps.html
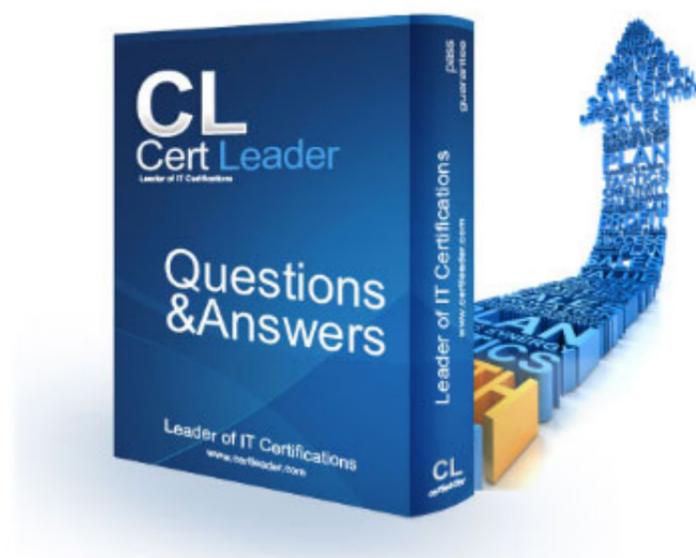
NEW QUESTION 1
A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification.
What is the MOST efficient way to meet these requirements?

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

Answer: B

NEW QUESTION 2
An application uses Amazon Cognito to manage end users' permissions when directly accessing AWS resources, including Amazon DynamoDB. A new feature request reads as follows:
Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.
The priorities are to reduce complexity and avoid potential for future security issues. Which approach will meet these requirements and priorities?

A. Create a new database field "suspended_status" and modify the application logic to validate that field when processing requests.
B. Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.
C. Use Amazon Cognito Sync to push out a "suspension_status" parameter and split the IAM policy into normal users and suspended users.
D. Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

Answer: D

NEW QUESTION 3
A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year.
What can be done to implement the above policy?

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

Answer: D

NEW QUESTION 4
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 forensics.

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 5
Your developer is using the KMS service and an assigned key in their Java program. They get the below error when running the code
arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey Which of the following could help resolve the issue?
Please select:

A. Ensure that UserB is given the right IAM role to access the key
B. Ensure that UserB is given the right permissions in the IAM policy
C. Ensure that UserB is given the right permissions in the Key policy
D. Ensure that UserB is given the right permissions in the Bucket policy

Answer: C

Explanation:
You need to ensure that UserB is given access via the Key policy for the Key C:\Users\wk\Desktop\mudassar\Untitled.jpg
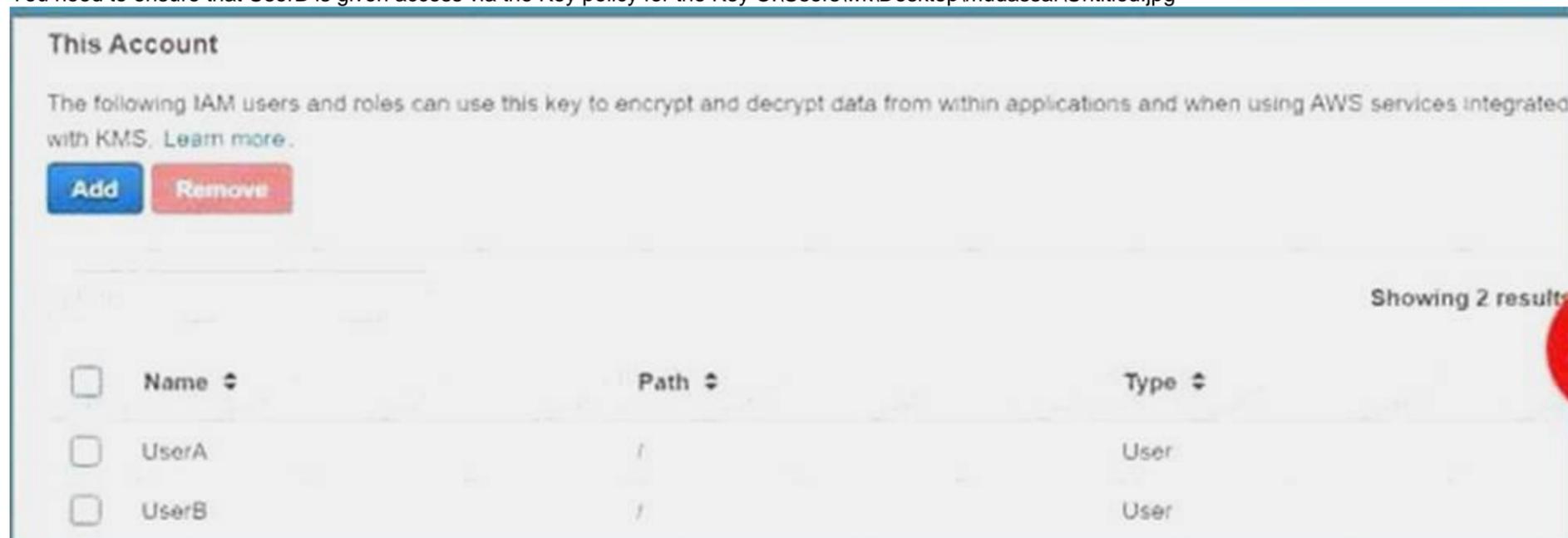
Option is invalid because you don't assign roles to 1AM users
For more information on Key policies please visit the below Link: https://docs.aws.amazon.com/kms/latest/developerguide/key-poli
The correct answer is: Ensure that UserB is given the right permissions in the Key policy

NEW QUESTION 6
A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:

≫ Encryption at rest

≫ Logging of all object retrievals in AWS CloudTrail
Which of the following meet these security requirements? (Choose three.)

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

Answer: ACE

NEW QUESTION 7
You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?
Please select:

A. AWS Cloudwatch
B. AWS EC2
C. AWS Trusted Advisor
D. AWS SNS

Answer: C

Explanation:
Below is a snapshot of the service limits that the Trusted Advisor can monitor C:\Users\wk\Desktop\mudassar\Untitled.jpg

Service	Limits
Amazon Elastic Compute Cloud (Amazon EC2)	Elastic IP addresses (EIPs)
	Reserved Instances - purchase limit (monthly)
Amazon Elastic Block Store (Amazon EBS)	Active volumes
	Active snapshots
	General Purpose (SSD) volume storage (GiB)
	Provisioned IOPS
	Provisioned IOPS (SSD) volume storage (GiB)
	Magnetic volume storage (GiB)
Amazon Kinesis Streams	Shards

Option A is invalid because even though you can monitor resources, it cannot be checked against the service limit.
Option B is invalid because this is the Elastic Compute cloud service Option D is invalid because it can be send notification but not check on service limit For more information on the Trusted Advisor monitoring, please visit the below URL:
https://aws.amazon.com/premiumsupport/ta-faqs> The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 8
A company has set up EC2 instances on the AW5 Cloud. There is a need to see all the IP addresses which are accessing the EC2 Instances. Which service can help achieve this?
Please select:

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

Answer: B

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

NEW QUESTION 9
Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?
Please select:

A. Enable MFA for these user accounts
B. Enable versioning for these user accounts
C. Enable accidental deletion for these user accounts
D. Disable root access for the users

Answer: A

Explanation:
The AWS Documentation mentions the following as a best practices for 1AM users. For extra security, enable multi-factor authentication (MFA) for privileged 1AM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).
Option B,C and D are invalid because no such security options are available in AWS For more information on 1AM best practices, please visit the below URL https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html The correct answer is: Enable MFA for these user accounts
Submit your Feedback/Queries to our Experts

NEW QUESTION 10
A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.
What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

A. Store the scripts in the AMI and encrypt the sensitive data using AWS KMS Use the instance role profile to control access to the KMS keys needed to decrypt the data.
B. Store the sensitive data in AWS Systems Manager Parameter Store using the encrypted string parameter and assign the GetParameters permission to the EC2 instance role.
C. Externalize the bootstrap scripts in Amazon S3 and encrypt them using AWS KM

D. Remove the scripts from the instance and clear the logs after the instance is configured.
E. Block user access of the EC2 instance's metadata service using IAM policie
F. Remove all scripts and clear the logs after execution.

Answer: A

NEW QUESTION 10
A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.
What would be the BEST way to reduce the potential impact of these attacks in the future?

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

Answer: C

NEW QUESTION 13
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 17
A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.
What is the SIMPLEST way to meet these requirements?

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

Answer: C

NEW QUESTION 20
You have a set of application , database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly. There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take?
Please select:

A. Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group
B. Check the Outbound security rules for the database security group I Check the inbound security rules for the application security group
C. Check the both the Inbound and Outbound security rules for the database security group Check the inbound security rules for the application security group
D. Check the Outbound security rules for the database security groupCheck the both the Inbound and Outbound security rules for the application security group

Answer: A

Explanation:
Here since the communication would be established inward to the database server and outward from the application server, you need to ensure that just the Outbound rules for application server security groups are checked. And then just the Inbound rules for database server security groups are checked.
Option B can't be the correct answer. It says that we need to check the outbound security group which is not needed.
We need to check the inbound for DB SG and outbound of Application SG. Because, this two group need to communicate with each other to function properly.
Option C is invalid because you don't need to check for Outbound security rules for the database security group
Option D is invalid because you don't need to check for Inbound security rules for the application security group
For more information on Security Groups, please refer to below URL:
The correct answer is: Check the Inbound security rules for the database security group Check the Outbound

security rules for the application security group Submit your Feedback/Queries to our Experts

NEW QUESTION 24
A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted."
The security solution must meet all of the following requirements:

> Each object must be encrypted using a unique key.

> AWS KMS must automatically rotate encryption keys annually.
Which of the following meets these requirements?

A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annuall
B. For the "Restricted" CMK, define the MFA policy within the key polic
C. Use S3 SSE-KMS to encrypt the objects.
D. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to tru
E. S3 can then use the grants to encrypt each object with a unique CMK.
F. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA polic
G. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
H. Create a CMK with unique imported key material for each data classification type, and rotate them annuall
I. For the "Restricted" key material, define the MFA policy in the key polic
J. Use S3 SSE-KMS to encrypt the objects.

Answer: A

NEW QUESTION 26
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 policy.

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 29
Your company makes use of S3 buckets for storing data. There is a company policy that all services should have logging enabled. How can you ensure that logging is always enabled for created S3 buckets in the AWS Account?
Please select:

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

Answer: B

Explanation:
This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers Example rule with configuration change trigger
1. You add the AWS Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.
Option A is invalid because AWS Inspector cannot be used to scan all buckets
Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets. For more information on Config Rules please see the below Link:

➤ https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
The correct answer is: Use AWS Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 33
A Security Architect is evaluating managed solutions for storage of encryption keys. The requirements are:
-Storage is accessible by using only VPCs.
-Service has tamper-evident controls.
-Access logging is enabled.
-Storage has high availability.
Which of the following services meets these requirements?

A. Amazon S3 with default encryption
B. AWS CloudHSM
C. Amazon DynamoDB with server-side encryption
D. AWS Systems Manager Parameter Store

Answer: B

NEW QUESTION 34
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.
C:\Users\wk\Desktop\mudassar\Untitled.jpg

```
{
  "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 36

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 41

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.
Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below
Please select:

A. A network ACL with a rule that allows outgoing traffic on port 443.
B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
D. A security group with a rule that allows outgoing traffic on port 443
E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeralports.
F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Answer: BD

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

NEW QUESTION 44
Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which three 1AM best practices should you consider implementing?
Please select:

A. Create individual 1AM users
B. Configure MFA on the root account and for privileged 1AM users
C. Assign 1AM users and groups configured with policies granting least privilege access
D. Ensure all users have been assigned and dre frequently rotating a password, access ID/secret key, andX.509 certificate

Answer: ABC

Explanation:
When you go to the security dashboard, the security status will show the best practices for initiating the first level of security.
C:\Users\wk\Desktop\mudassar\Untitled.jpg
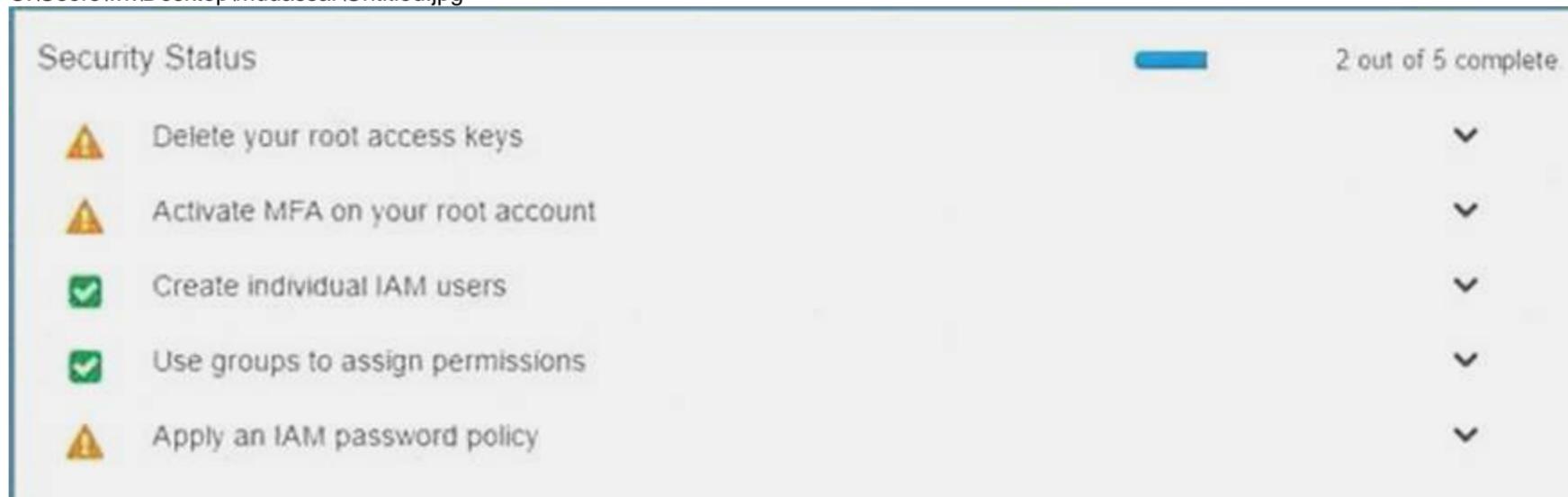
Option D is invalid because as per the dashboard, this is not part of the security recommendation For more information on best security practices please visit the URL:
https://aws.amazon.com/whitepapers/aws-security-best-practices;
The correct answers are: Create individual 1AM users, Configure MFA on the root account and for privileged 1AM users. Assign 1AM users and groups configured with policies granting least privilege access
Submit your Feedback/Queries to our Experts

NEW QUESTION 46
An organization has three applications running on AWS, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an AWS KMS Customer Master Key (CMK).
What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

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

Answer: B

NEW QUESTION 50
A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.
Which approach will meet these requirements while protecting the external certificate during a breach?

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

Answer: C

NEW QUESTION 53
A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.
Please select:

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

Answer: C

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

NEW QUESTION 58
An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.
Which of the following supports this requirement for AWS resources that are encrypted by AWS KMS?

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

Answer: C

NEW QUESTION 59
Your company is planning on developing an application in AWS. This is a web based application. The application users will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.
Please select:

A. Create an OIDC identity provider in AWS
B. Create a SAML provider in AWS
C. Use AWS Cognito to manage the user profiles
D. Use 1AM users to manage the user profiles

Answer: B

Explanation:
The AWS Documentation mentions the following The AWS Documentation mentions the following
OIDC identity providers are entities in 1AM that describe an identity provider (IdP) service that supports the OpenID Connect (OIDC) standard. You use an OIDC identity provider when you want to establish trust between an OIDC-compatible IdP—such as Google, Salesforce, and many others—and your AWS account This is useful if you are creating a mobile app or web application that requires access to AWS resources, but you don't want to create custom sign-in code or manage your own user identities
Option A is invalid because in the security groups you would not mention this information/ Option C is invalid because SAML is used for federated authentication
Option D is invalid because you need to use the OIDC identity provider in AWS For more information on ODIC identity providers, please refer to the below Link:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id roles providers create oidc.htmll
The correct answer is: Create an OIDC identity provider in AWS

NEW QUESTION 63
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 66
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 69
An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".
An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.
The IAM user policy is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            <Action>
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
            ]
            <CONDITION>
        }
    ]
}
```

What additional items need to be added to the IAM user policy? (Choose two.)

A. kms:GenerateDataKey
B. kms:Decrypt
C. kms:CreateGrant
D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonaws.com"}}
E. "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}

Answer: CE

NEW QUESTION 72
A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by AWS Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.
After a short period of time, a number of existing applications have failed with authentication errors. What is the MOST likely cause of the authentication errors?

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

Answer: B

NEW QUESTION 74
Your company has a set of EBS volumes defined in AWS. The security mandate is that all EBS volumes are encrypted. What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.
Please select:

A. Use AWS Inspector to inspect all the EBS volumes
B. Use AWS Config to check for unencrypted EBS volumes
C. Use AWS Guard duty to check for the unencrypted EBS volumes
D. Use AWS Lambda to check for the unencrypted EBS volumes

Answer: B

Explanation:
 The enc
config rule for AWS Config can be used to check for unencrypted volumes. encrypted-volurrn
5 volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryptio using the kmsld parameter, the rule checks if the EBS volumes in an attached state are encrypted with that KMS key*1.
Options A and C are incorrect since these services cannot be used to check for unencrypted EBS volumes Option D is incorrect because even though this is possible, trying to implement the solution alone with just the Lambda servk
would be too difficult
For more information on AWS Config and encrypted volumes, please refer to below URL: ⬧ https://docs.aws.amazon.com/config/latest/developerguide/encrypted-
volumes.html
Submit your Feedback/Queries to our Experts

NEW QUESTION 78
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 users.

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 80
A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events. How can this be achieved? Choose 2 answers from the options given below
Please select:

A. Create one Cloudtrail log group for data events
B. Create one trail that logs data events to an S3 bucket
C. Create another trail that logs management events to another S3 bucket
D. Create another Cloudtrail log group for management events

Answer: BC

Explanation:
The AWS Documentation mentions the following
You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket
Options A and D are invalid because you have to create a trail and not a log group

For more information on managing events with cloudtrail, please visit the following URL: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/loHEing-manasement-and-data-events-with-cloudtr The correct answers are: Create one trail that logs data events to an S3 bucket. Create another trail that logs management events to another S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 85
A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.
The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.
How can the Security Engineer address the issue?

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

Answer: B

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

NEW QUESTION 86
Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

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

Answer: A

NEW QUESTION 89
While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
What action should be performed to allow the ping to work?

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

Answer: B

NEW QUESTION 94
A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.
What is the MOST efficient way to meet these requirements?

A. Write an AWS Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.
B. Enable AWS CloudTrail logging for the AWS account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.
C. Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.
D. Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.

Answer: D

NEW QUESTION 97
A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.
What combination of actions should the Engineer take? (Choose two.)

A. Create an AWS Lambda function that determines whether Flow Logs are enabled for a given VPC.
B. Create an AWS Config configuration item for each VPC in the company AWS account.
C. Create an AWS Config managed rule with a resource type of AWS:: Lambda:: Function.
D. Create an Amazon CloudWatch Event rule that triggers on events emitted by AWS Config.
E. Create an AWS Config custom rule, and associate it with an AWS Lambda function that contains the evaluating logic.

Answer: AE

NEW QUESTION 99
A company has contracted with a third party to audit several AWS accounts. To enable the audit,
cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.
Which of the following may be causing this problem? (Choose three.)

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

Answer: ACF

NEW QUESTION 102
Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol.
There is a security mandate that all traffic between the client and the EC2 Instances need to be secure. How would you accomplish this?
Please select:

A. Use an Application Load balancer and terminate the SSL connection at the ELB
B. Use a Classic Load balancer and terminate the SSL connection at the ELB
C. Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
D. Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

Answer: D

Explanation:
Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the Ec2 Instances.
Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application. Option B is incorrect since encryption is required until the EC2 Instance
For more information on HTTPS listeners for classic load balancers, please refer to below URL
https://docs.aws.ama20n.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.htmll
The correct answer is: Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 103
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 106
A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.
Which solution would be MOST secure and easy to maintain?

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

Answer: C

NEW QUESTION 107
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
.a mazonaws.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 109
A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.
What configuration is necessary to allow the virtual security appliance to route the traffic?

A. Disable network ACLs.
B. Configure the security appliance's elastic network interface for promiscuous mode.
C. Disable the Network Source/Destination check on the security appliance's elastic network interface
D. Place the security appliance in the public subnet with the internet gateway

Answer: B

NEW QUESTION 112
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:
C:\Users\wk\Desktop\mudassar\Untitled.jpg

```
{
  "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 115
A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.
What is the MOST efficient way to manage access control for the KMS CMK7?

A. Use KMS grants to manage key acces
B. Programmatically create and revoke grants to manage vendor access.
C. Use an IAM role to manage key acces
D. Programmatically update the IAM role policies to manage vendor access.
E. Use KMS key policies to manage key acces
F. Programmatically update the KMS key policies to manage vendor access.
G. Use delegated access across AWS accounts by using IAM roles to manage key access.Programmatically update the IAM trust policy to manage cross-account vendor access.

Answer: A

NEW QUESTION 120
A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The Security team has the following requirements for the architecture:
• Data must be encrypted in transit.
• Data must be encrypted at rest.
• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Choose two.)

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

Answer: BC

Explanation:

Bucket encryption using KMS will protect both in case disks are stolen as well as if the bucket is public. This is because the KMS key would need to have privileges granted to it for users outside of AWS.

NEW QUESTION 122
A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is triggered whenever an object is stored within the S3 bucket.
How should the Lambda function be given access to the DynamoDB table?
Please select:

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

Answer: D

Explanation:
The ideal way is to create an 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 125
A company is using CloudTrail to log all AWS API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.
What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below
Please select:

A. Create an S3 bucket in a dedicated log account and grant the other accounts write only acces
B. Deliver all log files from every account to this S3 bucket.
C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
D. Run the function every 10 minutes.
E. Enable CloudTrail log file integrity validation
F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
G. Create a Security Group that blocks all traffic except calls from the CloudTrail servic
H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

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

NEW QUESTION 130
There is a requirement for a company to transfer large amounts of data between AWS and an on-premise location. There is an additional requirement for low latency and high consistency traffic to AWS. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below
Please select:

A. Provision a Direct Connect connection to an AWS region using a Direct Connect partner.
B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.
C. Create an iPSec tunnel for private connectivity, which increases network consistency and reduces latency.
D. Create a VPC peering connection between AWS and the Customer gateway.

Answer: A

Explanation:
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect you can establish private connectivity between AWS and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than Internet-based connections.
Options B and C are invalid because these options will not reduce network latency Options D is invalid because this is only used to connect 2 VPC's
For more information on AWS direct connect, just browse to the below URL: https://aws.amazon.com/directconnect
The correct answer is: Provision a Direct Connect connection to an AWS region using a Direct Connect partner. omit your Feedback/Queries to our Experts

NEW QUESTION 135
You have been given a new brief from your supervisor for a client who needs a web application set up on AWS. The a most important requirement is that MySQL must be used as the database, and this database must not be hosted in t« public cloud, but rather at the client's data center due to security risks. Which of the following solutions would be the ^ best to assure that the client's requirements are met? Choose the correct answer from the options below
Please select:

A. Build the application server on a public subnet and the database at the client's data cente
B. Connect them with a VPN connection which uses IPsec.
C. Use the public subnet for the application server and use RDS with a storage gateway to access and synchronize the data securely from the local data center.
D. Build the application server on a public subnet and the database on a private subnet with a NAT instance between them.
E. Build the application server on a public subnet and build the database in a private subnet with a secure ssh connection to the private subnet from the client's data center.

Answer: A

Explanation:
Since the database should not be hosted on the cloud all other options are invalid. The best option is to create a VPN connection for securing traffic as shown below. C:\Users\wk\Desktop\mudassar\Untitled.jpg
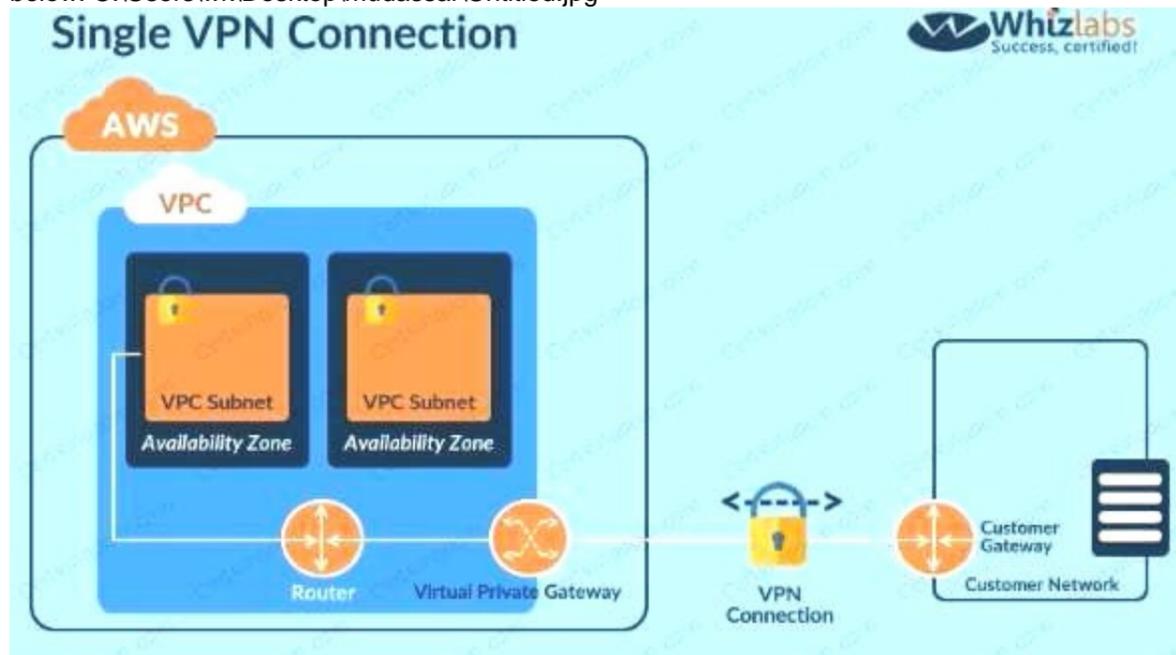
Option B is invalid because this is the incorrect use of the Storage gateway Option C is invalid since this is the incorrect use of the NAT instance Option D is invalid since this is an incorrect configuration For more information on VPN connections, please visit the below URL
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.htmll
The correct answer is: Build the application server on a public subnet and the database at the client's data center. Connect them with a VPN connection which uses IPsec
Submit your Feedback/Queries to our Experts

NEW QUESTION 139
You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly accessible from S3 directly?
Please select:

A. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
B. Add the CloudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
C. Create an Identity and Access Management (1AM) User for CloudFront and grant access to the objects in your S3 bucket to that 1AM User.
D. Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: A

Explanation:
You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it
To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.
Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.
Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.
For more information on serving private content via Cloudfront, please visit the following URL:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.htmll
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket t that OAI.
You can optionally secure the content in your Amazon S3 bucket so users can access it through CloudFront but cannot access it directly by using Amazon S3 URLs. This prevents anyone from bypassing CloudFront and using the Amazon S3 URL to get content that you want to restrict access to. This step isn't required to use signed URLs, but we recommend it

To require that users access your content through CloudFront URLs, you perform the following tasks: Create a special CloudFront user called an origin access identity.

Give the origin access identity permission to read the objects in your bucket. Remove permission for anyone else to use Amazon S3 URLs to read the objects.

Option B,C and D are all automatically invalid, because the right way is to ensure to create Origin Access Identity (OAI) for CloudFront and grant access accordingly.

For more information on serving private content via Cloudfront, please visit the following URL:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.htmll

The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket t that OAI.

Submit your Feedback/Queries to our Experts

Submit your Feedback/Queries to our Experts

NEW QUESTION 141
A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.
Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

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

Answer: CE

NEW QUESTION 143
A company wants to control access to its AWS resources by using identities and groups that are defined in its existing Microsoft Active Directory.
What must the company create in its AWS account to map permissions for AWS services to Active Directory user attributes?

A. AWS IAM groups
B. AWS IAM users
C. AWS IAM roles
D. AWS IAM access keys

Answer: C

NEW QUESTION 147
You company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes? Choose 2 answers from the options given below
Please select:

A. Use Windows bit locker for EBS volumes on Windows instances
B. Use TrueEncrypt for EBS volumes on Linux instances
C. Use AWS Systems Manager to encrypt the existing EBS volumes
D. Boot EBS volume can be encrypted during launch without using custom AMI

Answer: AB

Explanation:
EBS encryption can also be enabled when the volume is created and not for existing volumes. One can use existing tools for OS level encryption.
Option C is incorrect.
AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.
Option D is incorrect
You cannot choose to encrypt a non-encrypted boot volume on instance launch. To have encrypted boot volumes during launch , your custom AMI must have it's boot volume encrypted before launch.
For more information on the Security Best practices, please visit the following URL: com/whit Security Practices.
The correct answers are: Use Windows bit locker for EBS volumes on Windows instances. Use TrueEncrypt for EBS volumes on Linux instances
Submit your Feedback/Queries to our Experts

NEW QUESTION 151
An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer. There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses AWS WAF. The application is currently experiencing a volumetric attack whereby the attacker is exploiting a bug in a popular mobile game.
The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0)
What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

A. Create a rule in AWS WAF rules with conditions that block requests based on the presence of ExampleGame/1.22 in the User-Agent header
B. Create a geographic restriction on the CloudFront distribution to prevent access to the application from most geographic regions
C. Create a rate-based rule in AWS WAF to limit the total number of requests that the web application services.
D. Create an IP-based blacklist in AWS WAF to block the IP addresses that are originating from requests that contain ExampleGame/1.22 in the User-Agent header.

Answer: A

NEW QUESTION 152
Your company has many AWS accounts defined and all are managed via AWS Organizations. One AWS account has a S3 bucket that has critical data. How can we ensure that all the users in the AWS organisation have access to this bucket?
Please select:

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

Answer: A

Explanation:
The AWS Documentation mentions the following
AWS Identity and Access Management (1AM) now makes it easier for you to control access to your AWS resources by using the AWS organization of 1AM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, aws:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization
Option B.C and D are invalid because the condition in the bucket policy has to mention aws:PrincipalOrgID For more information on controlling access via Organizations, please refer to the below Link:
https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-usins-the-aws-organization-of-iam-p (
The correct answer is: Ensure the bucket policy has a condition which involves aws:PrincipalOrgID Submit your Feedback/Queries to our Experts

NEW QUESTION 153
You have enabled Cloudtrail logs for your company's AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?
Please select:

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

Answer: B

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

NEW QUESTION 158
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 ago.

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-aws-customers/ The correct answer is: Search the Cloudtrail event history on the API events which occurred 11 days ago.

NEW QUESTION 162
What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Choose two.)

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

Answer: BD

NEW QUESTION 163
Which of the following are valid event sources that are associated with web access control lists that trigger AWS WAF rules? (Choose two.)

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

Answer: BC

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

NEW QUESTION 166
An application outputs logs to a text file. The logs must be continuously monitored for security incidents. Which design will meet the requirements with MINIMUM effort?

A. Create a scheduled process to copy the component's logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log dat
B. Set up CloudWatch alerts based on the metrics.
C. Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instanc
D. Create a CloudWatch metric filter to monitor the application log
E. Set up CloudWatch alerts based on the metrics.
F. Create a scheduled process to copy the application log files to AWS CloudTrai
G. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log dat
H. Set up CloudWatch alerts based on the metrics.
I. Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file.Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log dat
J. Set up CloudWatch alerts based on the metrics.

Answer: B

NEW QUESTION 171
An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.
Which steps should be taken to troubleshoot the issue? (Choose two.)

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

Answer: AB

NEW QUESTION 175
Development teams in your organization use S3 buckets to store the log files for various applications hosted ir development environments in AWS. The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs. What feature will enable this requirement?
Please select:

A. Adding a bucket policy on the S3 bucket.
B. Configuring lifecycle configuration rules on the S3 bucket.
C. Creating an 1AM policy for the S3 bucket.
D. Enabling CORS on the S3 bucket.

Answer: B

Explanation:
The AWS Documentation mentions the following on lifecycle policies
Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified a« follows:
Transition actions - In which you define when objects transition to another . 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.
Expiration actions - In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.
Option A and C are invalid because neither bucket policies neither 1AM policy's can control the purging of logs Option D is invalid CORS is used for accessing objects across domains and not for purging of logs For more information on AWS S3 Lifecycle policies, please visit the following URL:
com/AmazonS3/latest/d<
The correct answer is: Configuring lifecycle configuration rules on the S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 176
An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.

How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

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

Answer: B

NEW QUESTION 178
In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement
Please select:

A. Transparent data encryption
B. SSL from your application
C. Data keys from AWS KMS
D. Data Keys from CloudHSM

Answer: B

Explanation:
This is mentioned in the AWS Documentation
You can use SSL from your application to encrypt a connection to a DB instance running MySQL MariaDB, Amazon Aurora, SQL Server, Oracle, or PostgreSQL.
Option A is incorrect since Transparent data encryption is used for data at rest and not in transit Options C and D are incorrect since keys can be used for encryption of data at rest
For more information on working with RDS and SSL, please refer to below URL:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html
The correct answer is: SSL from your application Submit your Feedback/Queries to our Experts

NEW QUESTION 183
Your company uses AWS to host its resources. They have the following requirements
1) Record all API calls and Transitions
2) Help in understanding what resources are there in the account
3) Facility to allow auditing credentials and logins
Which services would suffice the above requirements Please select:

A. AWS Inspector, CloudTrail, IAM Credential Reports
B. CloudTrai
C. IAM Credential Reports, AWS SNS
D. CloudTrail, AWS Config, IAM Credential Reports
E. AWS SQS, IAM Credential Reports, CloudTrail

Answer: C

Explanation:
You can use AWS CloudTrail to get a history of AWS API calls and related events for your account. This history includes calls made with the AWS Management Console, AWS Command Line Interface, AWS SDKs, and other AWS services.
Options A,B and D are invalid because you need to ensure that you use the services of CloudTrail, AWS Config, 1AM Credential Reports
For more information on Cloudtrail, please visit the below URL:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
AWS Config is a service that enables you to assess, audit and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, char management and operational troubleshooting.
For more information on the config service, please visit the below URL https://aws.amazon.com/config/
You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the AWS Management Console, the AWS SDKs and Command Line Tools, or the 1AM API.
For more information on Credentials Report, please visit the below URL:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id
credentials_getting-report.html
The correct answer is: CloudTrail, AWS Config, 1AM Credential Reports Submit your Feedback/Queries to our Experts

NEW QUESTION 187
You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.
Please select:

A. You have not explicitly given access via the key policy
B. You have not explicitly given access via the 1AM policy
C. You have not given access via the 1AM roles
D. You have not explicitly given access via 1AM users

Answer: A

Explanation:
By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explii update the default key policy for these keys.
Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys
For more information on upgrading key policies please visit the following URL: https://docs.aws.ama20n.com/kms/latest/developerguide/key-policy-upgrading.html

(
The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 190
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions.
A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

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

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

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

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

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 191
During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.
What could have been done to detect and automatically remediate the incident?

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

E. Then use a Lambda function to enable AWS CloudTrail and deactivate the root API keys.
F. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API key
G. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

Answer: B

NEW QUESTION 193
A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer.
Assuming that AWS Certificate Manager is used, how many certificates will need to be generated?

A. One in the US West (Oregon) region and one in the US East (Virginia) region.
B. Two in the US West (Oregon) region and none in the US East (Virginia) region.
C. One in the US West (Oregon) region and none in the US East (Virginia) region.
D. Two in the US East (Virginia) region and none in the US West (Oregon) region.

Answer: A

NEW QUESTION 196
A company maintains sensitive data in an Amazon S3 bucket that must be protected using an AWS KMS CMK. The company requires that keys be rotated automatically every year.
How should the bucket be configured?

A. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select an AWS-managed CMK.
B. Select Amazon S3-AWS KMS managed encryption keys (S3-KMS) and select a customer-managed CMK with key rotation enabled.
C. Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select a customer-managed CMK that has imported key material.
D. Select server-side encryption with AWS KMS-managed keys (SSE-KMS) and select an alias to an AWS-managed CMK.

Answer: B

NEW QUESTION 198
A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.
Which of the following requires the LEAST amount of configuration when implementing this approach?

A. Place each file into a different S3 bucke
B. Set the default encryption of each bucket to use a different AWS KMS customer managed key.
C. Put all the files in the same S3 bucke
D. Using S3 events as a trigger, write an AWS Lambda function to encrypt each file as it is added using different AWS KMS data keys.
E. Use the S3 encryption client to encrypt each file individually using S3-generated data keys
F. Place all the files in the same S3 bucke
G. Use server-side encryption with AWS KMS-managed keys (SSE-KMS) to encrypt the data

Answer: D

NEW QUESTION 199
A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?
Please select:

A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
B. Use a custom solution available in the AWS Marketplace
C. Use VPC Flow logs to detect the issues and flag them accordingly.
D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:
Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.
C:\Users\wk\Desktop\mudassar\Untitled.jpg
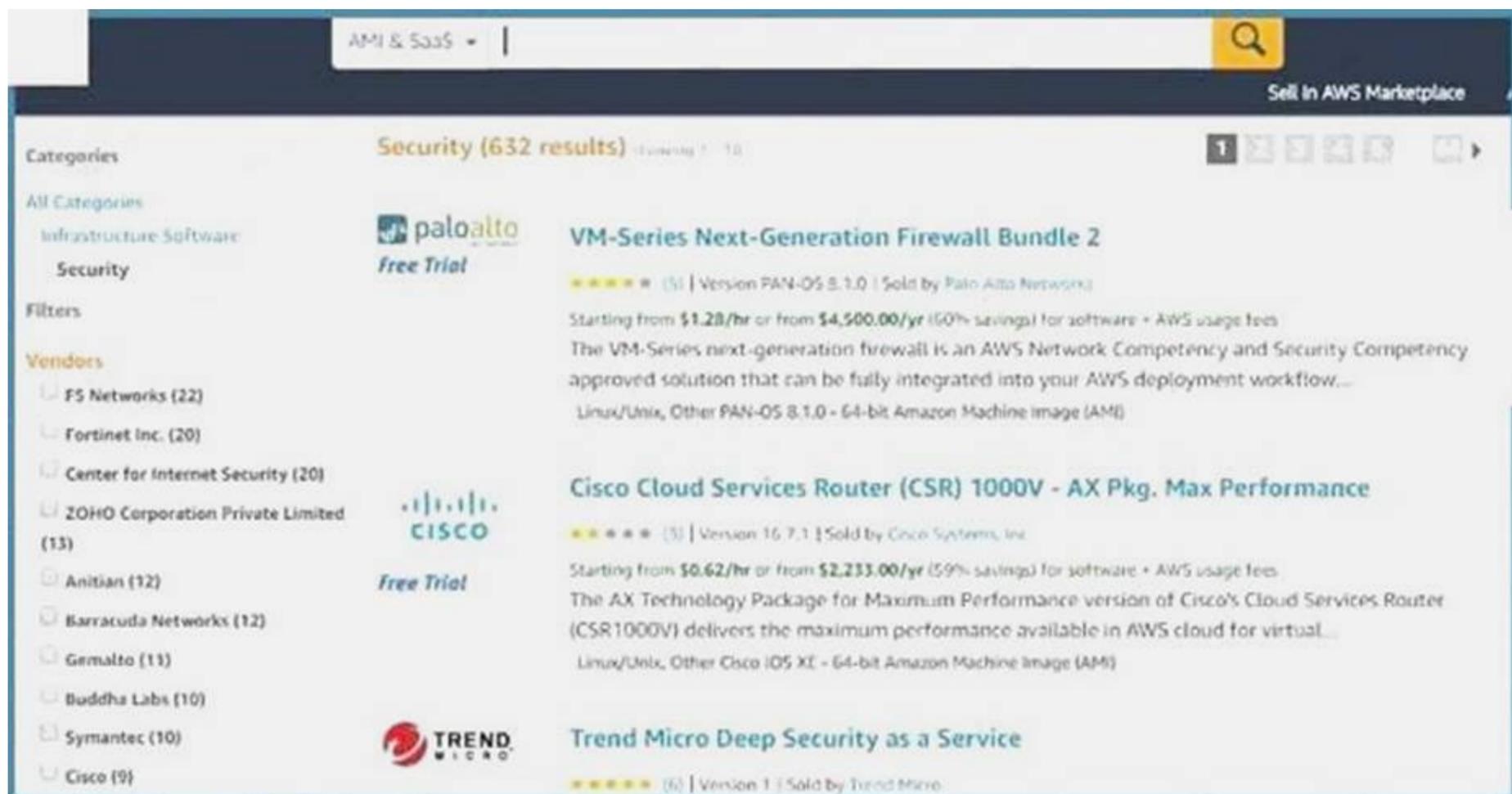
Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%200verview.pdf

For more information on using custom security solutions please visit the below URL: https://d1 .awsstatic.com/Marketplace/security/AWSMP Security Solution%20Overview.pd1

The correct answer is: Use a custom solution available in the AWS Marketplace Submit your Feedback/Queries to our Experts

NEW QUESTION 201
The Security Engineer created a new AWS Key Management Service (AWS KMS) key with the following key policy:

```
{
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:root"),
    "Action": "kms:*";
    "Resource": "*"
}
```

What are the effects of the key policy? (Choose two.)

A. The policy allows access for the AWS account 111122223333 to manage key access though IAM policies.
B. The policy allows all IAM users in account 111122223333 to have full access to the KMS key.
C. The policy allows the root user in account 111122223333 to have full access to the KMS key.
D. The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
E. The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Answer: BE

NEW QUESTION 203
A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?
Please select:

A. The user should use the same encryption key for all versions of the same object
B. It is possible to have different encryption keys for different versions of the same object
C. AWS S3 does not allow the user to upload his own keys for server side encryption
D. The SSE-C does not work when versioning is enabled

Answer: B

Explanation:
anaging your own encryption keys, y
You can encrypt the object and send it across to S3
Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use you own encryption keys Option D is invalid because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link:
""Keys.html https://docs.aws.ama2on.com/AmazonS3/latest/dev/UsingClientSideEncryption.html
The correct answer is: It is possible to have different encryption keys for different versions of the same object Submit your Feedback/Queries to our Experts

NEW QUESTION 204
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 205
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 exploits 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 208
An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.
How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.
B. Move the web servers to private subnets without public IP addresses.
C. Configure AWS WAF to provide DDoS attack protection for the ALB.
D. Require all inbound network traffic to route through a bastion host in the private subnet.
E. Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

Answer: BC

NEW QUESTION 211
A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below
Please select:

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

Answer: AD

Explanation:
Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.
Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk

For more information on AWS Security Groups, please visit the following UR https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-secunty.htmll
The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

NEW QUESTION 213
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 216
A company requires that data stored in AWS be encrypted at rest. Which of the following approaches achieve this requirement? Select 2 answers from the options given below.
Please select:

A. When storing data in Amazon EBS, use only EBS-optimized Amazon EC2 instances.
B. When storing data in EBS, encrypt the volume by using AWS KMS.
C. When storing data in Amazon S3, use object versioning and MFA Delete.
D. When storing data in Amazon EC2 Instance Store, encrypt the volume by using KMS.
E. When storing data in S3, enable server-side encryption.

Answer: BE

Explanation:
The AWS Documentation mentions the following
To create an encrypted Amazon EBS volume, select the appropriate box in the Amazon EBS section of the Amazon EC2 console. You can use a custom customer master key (CMK) by choosing one from the list that appears below the encryption box. If you do not specify a custom CMK, Amazon EBS uses the AWS-managed CMK for Amazon EBS in your account. If there is no AWS-managed CMK for Amazon EBS in your account, Amazon EBS creates one.
Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.
• Use Server-Side Encryption - You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
• Use Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.
Option A is invalid because using EBS-optimized Amazon EC2 instances alone will not guarantee protection of instances at rest. Option C is invalid because this will not encrypt data at rest for S3 objects. Option D is invalid because you don't store data in Instance store. For more information on EBS encryption, please visit the below URL:
https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html For more information on S3 encryption, please visit the below URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsinEEncryption.html
The correct answers are: When storing data in EBS, encrypt the volume by using AWS KMS. When storing data in S3, enable server-side encryption.
Submit your Feedback/Queries to our Experts

NEW QUESTION 217
You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?
Please select:

A. Use versioning and enable a timestamp for each version
B. Use Pre-signed URL's
C. Use 1AM Roles with a timestamp to limit the access
D. Use 1AM policies with a timestamp to limit the access

Answer: B

Explanation:
The AWS Documentation mentions the following
All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.
Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:
https://docs.aws.ama2on.com/AmazonS3/latest/dev/ShareObiectPreSisnedURL.html
The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 222
A company has set up the following structure to ensure that their S3 buckets always have logging enabled
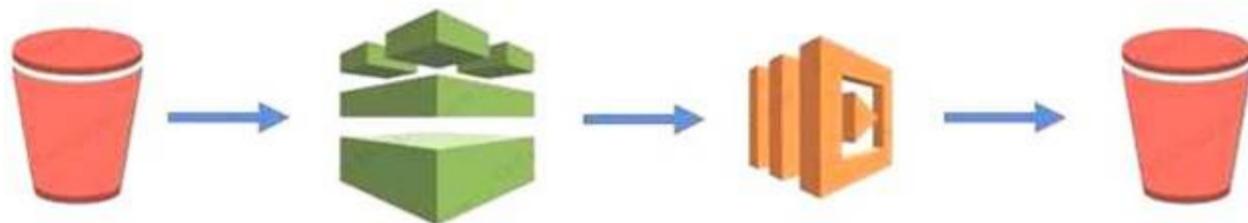
If there are any changes to the configuration to an S3 bucket, a config rule gets checked. If logging is disabled, then Lambda function is invoked. This Lambda function will again enable logging on the S3 bucket. Now there is an issue being encoutered with the entire flow. You have verified that the Lambda function is being invoked. But when logging is disabled for the bucket, the lambda function does not enable it again. Which of the following could be an issue
Please select:

A. The AWS Config rule is not configured properly
B. The AWS Lambda function does not have appropriate permissions for the bucket
C. The AWS Lambda function should use Node.js instead of python.
D. You need to also use the API gateway to invoke the lambda function

Answer: B

Explanation:
The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes. Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.
Option D is invalid because you don't necessarily need to use the API gateway service
For more information on accessing resources from a Lambda function, please refer to below URL https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.htmll
The correct answer is: The AWS Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 225
For compliance reasons, an organization limits the use of resources to three specific AWS regions. It wants to be alerted when any resources are launched in unapproved regions.
Which of the following approaches will provide alerts on any resources launched in an unapproved region?

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

Answer: A

NEW QUESTION 226
An AWS Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.
Which of the following explains why the logs are not available?

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

Answer: A

NEW QUESTION 227
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 230

Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?
Please select:

A. Use AWS inspector to consciously inspect the instances for port scans
B. Use AWS Trusted Advisor to notify of any malicious port scans
C. Use AWS Config to notify of any malicious port scans
D. Use AWS Guard Duty to monitor any malicious port scans

Answer: D

Explanation:
The AWS blogs mention the following to support the use of AWS GuardDuty
GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your AWS accounts. In combination with information gleaned from your VPC Flow Logs, AWS CloudTrail Event Logs, and DNS logs, th allows GuardDuty to detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the AWS side, it looks for suspicious AWS account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to AWS API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency.
Options A, B and C are invalid because these services cannot be used to detect port scans For more information on AWS Guard Duty, please refer to the below Link:
https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threat-detection; (
The correct answer is: Use AWS Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

NEW QUESTION 234

A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in AWS CloudTrail to support and troubleshoot the product.
Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

A. Ensure that the log file integrity validation mechanism is enabled.
B. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
C. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
D. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing—but not modifying—the log files.
E. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.

Answer: AD

NEW QUESTION 238

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

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

Answer: C

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

NEW QUESTION 242
......

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your SCS-C01 Exam with Our Prep Materials Via below:

https://www.certleader.com/SCS-C01-dumps.html