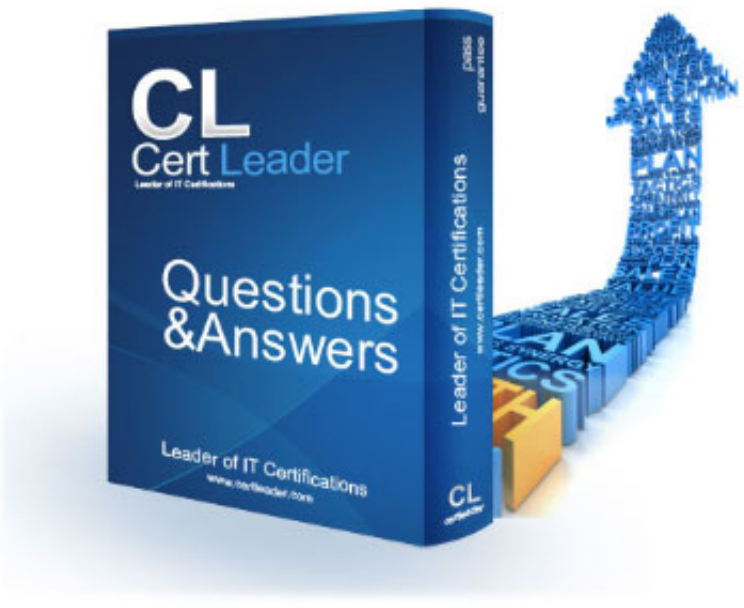
AWS-Certified-Security-Specialty Dumps

Amazon AWS Certified Security - Specialty

https://www.certleader.com/AWS-Certified-Security-Specialty-dumps.html



NEW QUESTION 1
You have a web site that is sitting behind AWS Cloudfront. You need to protect the web site against threats such as SQL injection and Cross site scripting attacks.
Which of the following service can help in such a scenario
Please select:

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

Answer: B

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

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

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

Answer: D

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

NEW QUESTION 3
When you enable automatic key rotation for an existing CMK key where the backing key is managed by AWS, after how long is the key rotated?
Please select:

A. After 30 days
B. After 128 days
C. After 365 days
D. After 3 years

Answer: D

Explanation:
The AWS Documentation states the following
• AWS managed CM Ks: You cannot manage key rotation for AWS managed CMKs. AWS KMS automatically rotates AWS managed keys every three years (1095 days).
Note: AWS-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365- days from when rotation is enabled.
Option A, B, C are invalid because the dettings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL
https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html
AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. This CMK is unique to your AWS account and region. Only the service that created the AWS managed CMK can use it
You can login to you 1AM dashbaord . Click on "Encryption Keys" You will find the list based on the services you are using as follows:
• aws/elasticfilesystem 1 aws/lightsail

• aws/s3
• aws/rds and many more Detailed Guide: KMS
You can recognize AWS managed CMKs because their aliases have the format aws/service-name, such as aws/redshift. Typically, a service creates its AWS managed CMK in your account when you set up the service or the first time you use the CMfC
The AWS services that integrate with AWS KMS can use it in many different ways. Some services create AWS managed CMKs in your account. Other services require that you specify a customer managed CMK that you have created. And, others support both types of CMKs to allow you the ease of an AWS managed CMK or the control of a customer-managed CMK
Rotation period for CMKs is as follows:
• AWS managed CMKs: 1095 days
• Customer managed CMKs: 365 days
Since question mentions about "CMK where backing keys is managed by AWS", its Amazon(AWS) managed and its rotation period turns out to be 1095 days{every 3 years)
For more details, please check below AWS Docs: https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html The correct answer is: After 3 years
Submit your Feedback/Queries to our Experts

NEW QUESTION 4
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.

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 5
Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved?
Please select:

A. Enable logging on the KMS service
B. Enable a trail in Cloudtrail
C. Enable Cloudwatch logs
D. Use Cloudwatch metrics

Answer: B

Explanation:
The AWS Documentation states the following
AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP
address from which the request was made, who made the request when it was made, and so on. Option A is invalid because logging is not possible in the KMS service
Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL
https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html The correct answer is: Enable a trail in Cloudtrail
Jubmit your Feedback/Queries to our Experts

NEW QUESTION 6
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 7
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-validationintro. 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-multipleaccounts. html
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 8
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 9
A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.
How can the security team fulfill these requirements?
Please select:

A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/server
B. Redeploy all out of compliance instances/servers using an AMI with the latest patches.

C. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
D. Use Systems Manager Patch Manger to install the missing patches.
E. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
F. Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
G. Use Trusted Advisor to generate the report of out of compliance instances/server
H. Use Systems Manger Patch Manger to install the missing patches.

Answer: B

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

NEW QUESTION 10
Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account.
Please select:

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

Answer: A

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

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

NEW QUESTION 10
A company is deploying a new web application on AWS. Based on their other web applications, they
anticipate being the target of frequent DDoS attacks. Which steps can the company use to protect their application? Select 2 answers from the options given below.
Please select:

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

Answer: BD

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

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

NEW QUESTION 13
A company has several Customer Master Keys (CMK), some of which have imported key material.

Each CMK must be rotated annually.
What two methods can the security team use to rotate each key? Select 2 answers from the options given below
Please select:

A. Enable automatic key rotation for a CMK
B. Import new key material to an existing CMK
C. Use the CLI or console to explicitly rotate an existing CMK
D. Import new key material to a new CMK; Point the key alias to the new CMK.
E. Delete an existing CMK and a new default CMK will be create

Answer: AD

Explanation:
The AWS Documentation mentions the following
Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually.
Rotating Keys Manually
You might want to create a newCMKand use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.
When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the sam CMK to decrypt the dat
A. As long as you keep both
the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.
Option B is invalid because you also need to point the key alias to the new key Option C is invalid because existing CMK keys cannot be rotated as they are
Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key
For more information on Key rotation please see the below Link: https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html
The correct answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK; Point the key alias to the new CMK.
Submit your Feedback/Queries to our Experts

NEW QUESTION 17
A company continually generates sensitive records that it stores in an S3 bucket. All objects in the bucket are encrypted using SSE-KMS using one of the company's CMKs. Company compliance policies require that no more than one month of data be encrypted using the same encryption key. What solution below will meet the company's requirements?
Please select:

A. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.
B. Configure the CMK to rotate the key material every month.
C. Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK, updates the S3 bucket to use thfl new CMK, and deletes the old CMK.
D. Trigger a Lambda function with a monthly CloudWatch event that rotates the key material in the CMK.

Answer: A

Explanation:
You can use a Lambda function to create a new key and then update the S3 bucket to use the new key. Remember not to delete the old key, else you will not be able to decrypt the documents stored in the S3 bucket using the older key.
Option B is incorrect because AWS KMS cannot rotate keys on a monthly basis
Option C is incorrect because deleting the old key means that you cannot access the older objects Option D is incorrect because rotating key material is not possible.
For more information on AWS KMS keys, please refer to below URL: https://docs.aws.amazon.com/kms/latest/developereuide/concepts.htmll
The correct answer is: Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.
Submit your Feedback/Queries to our Experts

NEW QUESTION 19
A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance. A Linux bastion host is used to apply schema updates to the database - administrators connect to the host via SSH from a corporate workstation. The following security groups are applied to the infrastructure-
* sgLB - associated with the ELB
* sgWeb - associated with the EC2 instances.
* sgDB - associated with the database
* sgBastion - associated with the bastion host Which security group configuration will allow the application to be secure and functional?
Please select: A.
sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastion
sgBastion: allow port 22 traffic from the corporate IP address range
B.
sgLB :aIlow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLB
sgBastion: allow port 22 traffic from the VPC IP address range C.
sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB
sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range D.
sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB
sgDB :al!ow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

A.

Answer: D

Explanation:
The Load Balancer should accept traffic on ow port 80 and 443 traffic from 0.0.0.0/0 The backend EC2 Instances should accept traffic from the Load Balancer
The database should allow traffic from the Web server
And the Bastion host should only allow traffic from a specific corporate IP address range Option A is incorrect because the Web group should only allow traffic from the Load balancer For more information on AWS Security Groups, please refer to below URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-

network-security.htmll
The correct answer is: sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB
sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range Submit your Feedback/Queries to our Experts

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

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

Answer: AC

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

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

NEW QUESTION 28
Which technique can be used to integrate AWS 1AM (Identity and Access Management) with an on Questions & Answers PDF P-63
premise LDAP (Lightweight Directory Access Protocol) directory service? Please select:

A. Use an 1AM policy that references the LDAP account identifiers and the AWS credentials.
B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
D. Use 1AM roles to automatically rotate the 1AM credentials when LDAP credentials are update

Answer: B

Explanation:
On the AWS Blog site the following information is present to help on this context
The newly released whitepaper. Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can access AWS by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access AWS resources.
Option A.C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign on.
For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL:
https://aws.amazon.eom/blogs/security/new-whitepaper-sinEle-sign-on-inteErating-aws-openldapand- shibboleth/l
The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP. Submit your Feedback/Queries to our Experts

NEW QUESTION 29
You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved?

Please select:

A. Add the keys to the backend distribution.
B. Add the keys to the S3 bucket
C. Create pre-signed URL's
D. Use AWS Access keys

Answer: C

Explanation:
Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket.
Option D is invalid because this is used for programmatic access to AWS resources
You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the AWS Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers) Topics
• Creating CloudFront Key Pairs for Your Trusted Signers
• Reformatting the CloudFront Private Key (.NET and Java Only)
• Adding Trusted Signers to Your Distribution
• Verifying that Trusted Signers Are Active (Optional) 1 Rotating CloudFront Key Pairs
To create signed URLs or signed cookies, you need at least one AWS account that has an active CloudFront key pair. This accou is known as a trusted signer. The trusted signer has two purposes:
• As soon as you add the AWS account ID for your trusted signer to your distribution, CloudFront starts to require that users us signed URLs or signed cookies to access your objects.
' When you create signed URLs or signed cookies, you use the private key from the trusted signer's key pair to sign a portion of the URL or the cookie. When someone requests a restricted object CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed.
For more information on Cloudfront private trusted content please visit the following URL:
• https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contenttrusted- s
The correct answer is: Create pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 34
A company has an existing AWS account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company. What must be now done to secure the account. Choose 3 answers from the options given below.
Please select:

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

Answer: CDE

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

NEW QUESTION 37
Your company has created a set of keys using the AWS KMS service. They need to ensure that each key is only used for certain services. For example , they want one key to be used only for the S3 service. How can this be achieved?
Please select:

A. Create an 1AM policy that allows the key to be accessed by only the S3 service.
B. Create a bucket policy that allows the key to be accessed by only the S3 service.
C. Use the kms:ViaService condition in the Key policy
D. Define an 1AM user, allocate the key and then assign the permissions to the required service

Answer: C

Explanation:
Option A and B are invalid because mapping keys to services cannot be done via either the 1AM or bucket policy
Option D is invalid because keys for 1AM users cannot be assigned to services This is mentioned in the AWS Documentation
The kms:ViaService condition key limits use of a customer-managed CMK to requests from particular AWS services. (AWS managed CMKs in your account, such as aws/s3, are always restricted to the AWS service that created them.)
For example, you can use kms:V1aService to allow a user to use a customer managed CMK only for requests that Amazon S3 makes on their behalf. Or you can use it to deny the user permission to a CMK when a request on their behalf comes from AWS Lambda.
For more information on key policy's for KMS please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/policy-conditions.html
The correct answer is: Use the kms:ViaServtce condition in the Key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 42
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 44
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 48
Which of the following is the responsibility of the customer? Choose 2 answers from the options given below.
Please select:

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

Answer: BC

Explanation:

Below is the snapshot of the Shared Responsibility Model

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

NEW QUESTION 49
You have just developed a new mobile application that handles analytics workloads on large scale datasets that are stored on Amazon Redshift. Consequently, the application needs to access Amazon Redshift tables. Which of the belov methods would be the best both practically and security-wise, to access the tables?
Choose the correct answer from the options below
Please select:

A. Create an 1AM user and generate encryption keys for that use
B. Create a policy for Redshift readonly acces
C. Embed th keys in the application.
D. Create an HSM client certificate in Redshift and authenticate using this certificate.
E. Create a Redshift read-only access policy in 1AM and embed those credentials in the application.
F. Use roles that allow a web identity federated user to assume a role that allows access to the Redshift table by providing temporary credentials.

Answer: D

Explanation:
The AWS Documentation mentions the following
"When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads t device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamica when needed using web
identify federation. The supplied temporary credentials map to an AWS role that has only the permissioi needed to perform the tasks required by the mobile app".
Option A.B and C are all automatically incorrect because you need to use 1AM Roles for Secure access to services For more information on web identity federation please refer to the below Link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html
The correct answer is: Use roles that allow a web identity federated user to assume a role that allows access to the RedShift table by providing temporary credentials.
Submit your Feedback/Queries to our Experts

NEW QUESTION 50

Your team is designing a web application. The users for this web application would need to sign in via an external ID provider such asfacebook or Google. Which of the following AWS service would you use for authentication?
Please select:

A. AWS Cognito
B. AWS SAML
C. AWS 1AM
D. AWS Config

Answer: A

Explanation:
The AWS Documentation mentions the following
Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users ca sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.
Option B is incorrect since this is used for identity federation
Option C is incorrect since this is pure Identity and Access management Option D is incorrect since AWS is a configuration service
For more information on AWS Cognito please refer to the below Link: https://docs.aws.amazon.com/coenito/latest/developerguide/what-is-amazon-cognito.html
The correct answer is: AWS Cognito
Submit your Feedback/Queries to our Experts

NEW QUESTION 54
Your application currently use AWS Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How wou you manage the access effectively?
Please select:

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

Answer: B

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

NEW QUESTION 57
Your company has a hybrid environment, with on-premise servers and servers hosted in the AWS cloud. They are planning to use the Systems Manager for patching servers. Which of the following is a pre-requisite for this to work;
Please select:

A. Ensure that the on-premise servers are running on Hyper-V.
B. Ensure that an 1AM service role is created
C. Ensure that an 1AM User is created
D. Ensure that an 1AM Group is created for the on-premise servers

Answer: B

Explanation:
You need to ensure that an 1AM service role is created for allowing the on-premise servers to communicate with the AWS Systems Manager.
Option A is incorrect since it is not necessary that servers should only be running Hyper-V Options C and D are incorrect since it is not necessary that 1AM users and groups are created For more information on the Systems Manager role please refer to the below URL:
.com/systems-rnanaeer/latest/usereuide/sysman-!
The correct answer is: Ensure that an 1AM service role is created Submit your Feedback/Queries to our Experts

NEW QUESTION 58
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 62
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-dataevents- with-cloudtrai
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 63
Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following
Whether any ports are left open other than admin ones like SSH and RDP
Whether any ports to the database server other than ones from the web server security group are
open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?
Please select:

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

Answer: B

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

NEW QUESTION 66
Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below
Please select:

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

Answer: AC

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

The correct answers are: AWS Cloudfront AWS Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 67
The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned 1AM policy statements allows the user to have access to the AWS usage report page?
Please select:

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

Answer: C

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

NEW QUESTION 72
There is a set of Ec2 Instances in a private subnet. The application hosted on these EC2 Instances need to access a DynamoDB table. It needs to be ensured that traffic does not flow out to the internet. How can this be achieved?
Please select:

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

Answer: A

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

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

NEW QUESTION 75
You need to establish a secure backup and archiving solution for your company, using AWS. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which AWS service fulfills these requirements in the most cost-effective way?
Choose the correct answer
Please select:

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

D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

Answer: A

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

NEW QUESTION 78
A company is planning on using AWS EC2 and AWS Cloudfrontfor their web application. For which one of the below attacks is usage of Cloudfront most suited for?
Please select:

A. Cross side scripting
B. SQL injection
C. DDoS attacks
D. Malware attacks

Answer: C

Explanation:
The below table from AWS shows the security capabilities of AWS Cloudfront AWS Cloudfront is more prominent for DDoS attacks.

Options A,B and D are invalid because Cloudfront is specifically used to protect sites against DDoS attacks For more information on security with Cloudfront, please refer to the below Link: https://d1.awsstatic.com/whitepapers/Security/Secure content delivery with CloudFront whitepaper.pdi
The correct answer is: DDoS attacks
Submit your Feedback/Queries to our Experts

NEW QUESTION 81
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-threatdetection; (
The correct answer is: Use AWS Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

NEW QUESTION 83

You have an Amazon VPC that has a private subnet and a public subnet in which you have a NAT instance server. You have created a group of EC2 instances that configure themselves at startup by downloading a bootstrapping script
from S3 that deploys an application via GIT.
Which one of the following setups would give us the highest level of security? Choose the correct answer from the options given below.
Please select:

A. EC2 instances in our public subnet, no EIPs, route outgoing traffic via the IGW
B. EC2 instances in our public subnet, assigned EIPs, and route outgoing traffic via the NAT
C. EC2 instance in our private subnet, assigned EIPs, and route our outgoing traffic via our IGW
D. EC2 instances in our private subnet, no EIPs, route outgoing traffic via the NAT

Answer: D

Explanation:
The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.

Options A and B are invalid because the instances need to be in the private subnet
Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance
For more information on NAT instance, please refer to the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC lnstance.html!
The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

NEW QUESTION 86
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 91
Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?
Please select:

A. Enable VPC flow logs to know the source IP addresses
B. Monitor the S3 API calls by using Cloudtrail logging
C. Monitor the S3 API calls by using Cloudwatch logging
D. Enable AWS Inspector for the S3 bucket

Answer: B

Explanation:
The AWS Documentation mentions the following
Amazon S3 is integrated with AWS CloudTrail. CloudTrail is a service that captures specific API calls made to Amazon S3 from your AWS account and delivers the log files to an Amazon S3 bucket that you specify. It captures API calls made from the Amazon S3 console or from the Amazon S3 API. Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request when it was
made, and so on
Options A,C and D are invalid because these services cannot be used to get the source IP address of the calls to S3 buckets
For more information on Cloudtrail logging, please refer to the below Link:
https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logeins.htmll
The correct answer is: Monitor the S3 API calls by using Cloudtrail logging Submit your Feedback/Queries to our Experts

NEW QUESTION 93
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, and X.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.

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 94
A company is hosting sensitive data in an AWS S3 bucket. It needs to be ensured that the bucket always remains private. How can this be ensured continually?
Choose 2 answers from the options given below
Please select:

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

Answer: AD

Explanation:
One of the AWS Blogs mentions the usage of AWS Config and Lambda to achieve this. Below is the diagram representation of this

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

and-respond-toamazon- s3-buckets-allowinj
The correct answers are: Use AWS Config to monitor changes to the AWS Bucket Use AWS Lambda function to change the bucket ACL

NEW QUESTION 96
You have an EC2 instance with the following security configured:
1. ICMP inbound allowed on Security Group
2. ICMP outbound not configured on Security Group
3. ICMP inbound allowed on Network ACL
4. ICMP outbound denied on Network ACL
If Flow logs is enabled for the instance, which of the following flow records will be recorded? Choose 3 answers from the options give below
Please select:

A. An ACCEPT record for the request based on the Security Group
B. An ACCEPT record for the request based on the NACL
C. A REJECT record for the response based on the Security Group
D. A REJECT record for the response based on the NACL

Answer: ABD

Explanation:
This example is given in the AWS documentation as well
For example, you use the ping command from your home computer (IP address is 203.0.113.12) to your instance (the network interface's private IP address is 172.31.16.139). Your security group's inbound rules allow ICMP traffic and the outbound rules do not allow ICMP traffic however, because security groups are stateful, the response ping from your instance is allowed. Your network ACL permits inbound ICMP traffic but does not permit outbound ICMP traffic. Because network ACLs are stateless, the response ping is dropped and will not reach your home computer. In a flow log, this is displayed as 2 flow log records:
An ACCEPT record for the originating ping that was allowed by both the network ACL and the security group, and therefore was allowed to reach your instance.
A REJECT record for the response ping that the network ACL denied.
Option C is invalid because the REJECT record would not be present For more information on Flow Logs, please refer to the below URL:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-loes.html
The correct answers are: An ACCEPT record for the request based on the Security Group, An ACCEPT record for the request based on the NACL, A REJECT record for the response based on the NACL Submit your Feedback/Queries to our Experts

NEW QUESTION 101
Your company has a set of EC2 Instances defined in AWS. These Ec2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly. How can you achieve this?
Please select:

A. Use Cloudwatch logs to monitor the activity on the Security Group
B. Use filters to search for the changes and use SNS for the notification.
C. Use Cloudwatch metrics to monitor the activity on the Security Group
D. Use filters to search for the changes and use SNS for the notification.
E. Use AWS inspector to monitor the activity on the Security Group
F. Use filters to search for the changes and use SNS f the notification.
G. Use Cloudwatch events to be triggered for any changes to the Security Group
H. Configure theLambda function for email notification as wel

Answer: D

Explanation:
The below diagram from an AWS blog shows how security groups can be monitored

Option A is invalid because you need to use Cloudwatch Events to check for chan, Option B is invalid because you need to use Cloudwatch Events to check for chang
Option C is invalid because AWS inspector is not used to monitor the activity on Security Groups For more information on monitoring security groups, please visit the below URL: lhttpsy/aws.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notificationsabout- changes-to-your-amazonj 'pc-security-groups/
The correct answer is: Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.
Submit your Feedback/Queries to our Experts

NEW QUESTION 104
Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement.
Please select:

A. Set up VPC peering between the central server VPC and each of the teams VPCs.
B. Set up AWS DirectConnect between the central server VPC and each of the teams VPCs.
C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.
D. None of the above options will work.

Answer: A

Explanation:
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region. Options B and C are invalid because you need to use VPC Peering
Option D is invalid because VPC Peering is available
For more information on VPC Peering please see the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html
The correct answer is: Set up VPC peering between the central server VPC and each of the teams VPCs. Submit your Feedback/Queries to our Experts

NEW QUESTION 107

There is a requirement for a company to transfer large amounts of data between AWS and an onpremise 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 gatewa

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 InternetQuestions
& Answers PDF P-140 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 108
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 111
Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?
Please select:

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

Answer: A

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

NEW QUESTION 114
There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address

block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's.
Please select:

A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.
B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.
C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.
D. Modify the Windows Firewall settings on all AMI'S that your organization uses in that VPC to deny access from the IP address block.

Answer: B

Explanation:
NACL acts as a firewall at the subnet level of the VPC and we can deny the offending IP address block
at the subnet level using NACL rules to block the incoming traffic to the VPC instances. Since NACL rules are applied as per the Rule numbers make sure that this rule number should take precedence over other rule numbers if there are any such rules that will allow traffic from these IP ranges. The lowest rule number has more precedence over a rule that has a higher number.
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 a 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). Options C is invalid because these options are not available
Option D is invalid because there is not root access for users
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: Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.
omit your Feedback/Queries to our Experts

NEW QUESTION 116
.....

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 AWS-Certified-Security-Specialty Exam with Our Prep Materials Via below:

https://www.certleader.com/AWS-Certified-Security-Specialty-dumps.html