AWS-Certified-Security-Specialty Dumps

Amazon AWS Certified Security - Specialty

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

NEW QUESTION 1

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP. How can you protect the subnets from this attack?
Please select:

A. Change the Inbound Security Groups to deny access from the suspecting IP
B. Change the Outbound Security Groups to deny access from the suspecting IP
C. Change the Inbound NACL to deny access from the suspecting IP
D. Change the Outbound NACL to deny access from the suspecting IP

Answer: C

Explanation:
Option A and B are invalid because by default the Security Groups already block traffic. You can use NACL's as an additional security layer for the subnet to deny traffic.
Option D is invalid since just changing the Inbound Rules is sufficient The AWS Documentation mentions the following
A network access control list (ACLJ is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.
The correct answer is: Change the Inbound NACL to deny access from the suspecting IP

NEW QUESTION 2

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 3

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 4

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 5
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 6
You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.
Please select:

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

Answer: AB

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

NEW QUESTION 7
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%20Overview.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 8
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 9
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 10
You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?
Please select:

A. Shutdown the instance
B. Remove the rule for incoming traffic on port 22 for the Security Group
C. Change the AMI for the instance
D. Change the Instance type for the instance

Answer: B

Explanation:
In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.
Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.
For more information on authorizing access to an instance, please visit the below URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.htmll The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

NEW QUESTION 10
Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

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

Answer: C

Explanation:
This concept is given in the AWS Documentation
How do I submit a penetration testing request for my AWS resources? Issue
I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?
Resolution
Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.
AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.
If your request is approved, you'll receive an authorization number.
Option A.B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests
For more information on penetration testing, please visit the below URL
* https://aws.amazon.com/security/penetration-testing/
* https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/ (
The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

NEW QUESTION 11
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 14
You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.
Please select:

A. Use the AWS Trusted Advisor to see what can be done.
B. Use VPC Flow logs to diagnose the traffic
C. Use AWS WAF to analyze the traffic
D. Use AWS Guard Duty to analyze the traffic

Answer: B

Explanation:
Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application
Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application
Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application
The AWS Documentation mentions the following
VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security toi to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.
For more information on AWS Security, please visit the following URL: https://aws.amazon.com/answers/networking/vpc-security-capabilities>
The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

NEW QUESTION 19
A company hosts a critical web application on the AWS Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?
Please select:

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

Answer: C

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

NEW QUESTION 20
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 ephemeral ports.
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 21
Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances. Which of the following would be an effective way to achieve this?
Please select:

A. Use the AWS Systems Manager Parameter Store
B. Use the AWS Systems Manager Run Command
C. Use the AWS Inspector
D. Use AWS Config

Answer: B

Explanation:
The AWS Documentation mentions the following
AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.
Option A is invalid because this service is used to store parameter Option C is invalid because this service is used to scan vulnerabilities in an EC2 Instance.
Option D is invalid because this service is used to check for configuration changes For more information on executing remote commands, please visit the below U
https://docs.aws.amazon.com/systems-manaEer/latest/usereuide/execute-remote-commands.htmll (
The correct answer is: Use the AWS Systems Manager Run Command Submit your Feedback/Queries to our Experts

NEW QUESTION 26
You have a set of Keys defined using the AWS KMS service. You want to stop using a couple of keys , but are not sure of which services are currently using the keys. Which of the following would be a
safe option to stop using the keys from further usage. Please select:

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

Answer: B

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

NEW QUESTION 30
A company has external vendors that must deliver files to the company. These vendors have crossaccount that gives them permission to upload objects to one of the company's S3 buckets.
What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below
Please select:

A. Attach an 1AM role to the bucket that grants the bucket owner full permissions to the object
B. Add a grant to the objects ACL giving full permissions to bucket owner.
C. Encrypt the object with a KMS key controlled by the company.
D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object
E. Upload the file to the company's S3 bucket

Answer: BE

Explanation:
This scenario is given in the AWS Documentation
A bucket owner can enable other AWS accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.

Option A and D are invalid because bucket ACL's are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link:
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroushs-manaeing-accessexample3. htmll
The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the file to the company's S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 35
Your current setup in AWS consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server. Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup
Please select:

A. Consider moving the web server to a private subnet
B. Consider moving the database server to a private subnet
C. Consider moving both the web and database server to a private subnet
D. Consider creating a private subnet and adding a NAT instance to that subnet

Answer: B

Explanation:
The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet. The below diagram from the AWS Documentation shows how this can be setup

Option A and C are invalid because if you move the web server to a private subnet, then it cannot be accessed by users Option D is invalid because NAT instances should be present in the public subnet For more information on public and private subnets in AWS, please visit the following url
.com/AmazonVPC/latest/UserGuide/VPC Scenario2.
The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

NEW QUESTION 39
Your company has confidential documents stored in the simple storage service. Due to compliance requirements, you have to ensure that the data in the S3 bucket is available in a different geographical location. As an architect what is the change you would make to comply with this requirement.
Please select:

A. Apply Multi-AZ for the underlying 53 bucket
B. Copy the data to an EBS Volume in another Region
C. Create a snapshot of the S3 bucket and copy it to another region
D. Enable Cross region replication for the S3 bucket

Answer: D

Explanation:
This is mentioned clearly as a use case for S3 cross-region replication
You might configure cross-region replication on a bucket for various reasons, including the following:
• Compliance requirements - Although, by default Amazon S3 stores your data across multiple geographically distant Availability Zones, compliance requirements might dictate that you store data at even further distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these compliance requirements.
Option A is invalid because Multi-AZ cannot be used to S3 buckets
Option B is invalid because copying it to an EBS volume is not a recommended practice Option C is invalid because creating snapshots is not possible in S3
For more information on S3 cross-region replication, please visit the following URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.htmll
The correct answer is: Enable Cross region replication for the S3 bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 41
When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users? These permissions should be easily managed.
Please select:

A. Use the secure token service to manage the permissions for the different users
B. Use 1AM Policies to create different policies for the different types of users.
C. Use the AWS Config tool to manage the permissions for the different users
D. Use 1AM Access Keys to create sets of keys for the different types of user

Answer: B

Explanation:
The AWS Documentation mentions the following
You control access to Amazon API Gateway with 1AM permissions by controlling access to the following two API Gateway component processes:
* To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
* To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required 1AM actions supported by the API execution component of API Gateway.
Option A, C and D are invalid because these cannot be used to control access to AWS services. This needs to be done via policies. For more information on permissions with the API gateway, please visit the following URL: https://docs.aws.amazon.com/apisateway/latest/developerguide/permissions.html
The correct answer is: Use 1AM Policies to create different policies for the different types of users. Submit your Feedback/Queries to our Experts

NEW QUESTION 42
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 43
Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers. The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure. What process will check compliance of the company's EC2 instances?
Please select:

A. Trigger an AWS Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.
B. Query the Trusted Advisor API for all best practice security checks and check for "action recommened" status.
C. Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance.
D. Run an Amazon inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.

Answer: D

Explanation:
Option B is incorrect because querying Trusted Advisor API's are not possible
Option C is incorrect because GuardDuty should be used to detect threats and not check the compliance of security protocols.
Option D states that Run Amazon Inspector using runtime behavior analysis rules which will analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.
Insecure Server Protocols
This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.
For more information, please refer to below URL: https://docs.aws.amazon.eom/mspector/latest/userguide/inspector_runtime-behavioranalysis. html#insecure-protocols
(
The correct answer is: Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.
Submit your Feedback/Queries to our Experts

NEW QUESTION 45
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 :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 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 50
A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working. What is the other step that needs to be followed to ensure that the AD domain join can work as intended
Please select:

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

Answer: C

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

NEW QUESTION 53
You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?
Please select:

A. AWS KMS
B. AWS S3 Server side encryption
C. AWS Customer Keys
D. AWS Cloud HSM

Answer: B

Explanation:
The AWS Documentation mentions the following
Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using AWS S3 Server side encryption, AWS will manage the rotation of keys automatically.
For more information on Server side encryption, please visit the following URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsineServerSideEncryption.htmll
The correct answer is: AWS S3 Server side encryption Submit your Feedback/Queries to our Experts

NEW QUESTION 57
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 60
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 61
You are trying to use the AWS Systems Manager run command on a set of Instances. The run command on a set of Instances. What can you do to diagnose the issue? Choose 2 answers from the options given
Please select:

A. Ensure that the SSM agent is running on the target machine
B. Check the /var/log/amazon/ssm/errors.log file
C. Ensure the right AMI is used for the Instance
D. Ensure the security groups allow outbound communication for the instance

Answer: AB

Explanation:
The AWS Documentation mentions the following
If you experience problems executing commands using Run Command, there might be a problem with the SSM Agent. Use the following information to help you troubleshoot the agent
View Agent Logs
The SSM Agent logs information in the following files. The information in these files can help you troubleshoot problems.
On Windows
%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log
%PROGRAMDATA%\Amazon\SSM\Logs\error.log
The default filename of the seelog is seelog-xml.template. If you modify a seelog, you must rename the file to seelog.xml.
On Linux
/var/log/amazon/ssm/amazon-ssm-agentlog /var/log/amazon/ssm/errors.log
Option C is invalid because the right AMI has nothing to do with the issues. The agent which is used to execute run commands can run on a variety of AMI'S
Option D is invalid because security groups does not come into the picture with the communication between the agent and the SSM service
For more information on troubleshooting AWS SSM, please visit the following URL: https://docs.aws.amazon.com/systems-manaeer/latest/userguide/troubleshootine-remotecommands. htmll
The correct answers are: Ensure that the SSM agent is running on the target machine. Check the /var/log/amazon/ssm/errors.log file
Submit your Feedback/Queries to our Experts

NEW QUESTION 63
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 66
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: AExplanation:

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 67

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 71

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 73

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 77

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either

AWS Key Management Servic (AWS KMS) or a hardware security module (HSM) to manage the toplevel

encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.

Option A is invalid because its the cluster that needs to be encrypted

Option C is invalid because this encrypts objects in transit and not objects at rest Option D is invalid because this is used only for objects in S3 buckets

For more information on Redshift encryption, please visit the following URL: https://docs.aws.amazon.com/redshift/latest/memt/workine-with-db-encryption.htmll

The correct answer is: Use AWS KMS Customer Default master key Submit your Feedback/Queries to our Experts

NEW QUESTION 82

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result you will receive log files containing API activity for the new region without taking any action.

Option A and C is invalid because this would be a maintenance overhead to enable cloudtrail for every region

Option D is invalid because this AWS Config cannot be used to enable trails For more information on this feature, please visit the following URL: https://aws.ama2on.com/about-aws/whats-new/20l5/l2/turn-on-cloudtrail-across-all-reeions-andsupport- for-multiple-trails

The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

NEW QUESTION 85

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 89

One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance.

Select 2 answers from the options given below

Please select:

A. Remove the role applied to the Ec2 Instance
B. Create a separate forensic instance

C. Ensure that the security groups only allow communication to this forensic instance
D. Terminate the instance

Answer: BC

Explanation:
Option A is invalid because removing the role will not help completely in such a situation
Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance
One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance.
For more information on security scenarios for your EC2 Instance, please refer to below URL: https://d1.awsstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pd1
The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 93
One of your company's EC2 Instances have been compromised. The company has strict po thorough investigation on finding the culprit for the security breach. What would you do in from the options given below.
Please select:

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

Answer: ABC

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

NEW QUESTION 96
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 98
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 99
A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resource? for their infrastructure. They want to ensure that the EC2 Instances don't have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?
Please select:

A. Use AWS Config to check the state of the EC2 instance for any sort of security issues.
B. Use AWS Inspector API's in the pipeline for the EC2 Instances
C. Use AWS Trusted Advisor API's in the pipeline for the EC2 Instances
D. Use AWS Security Groups to ensure no vulnerabilities are present

Answer: B

Explanation:
Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple. DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre-existing issues or when new issues are introduced. Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the AWS Inspector service.
For more information on AWS Security best practices, please refer to below URL: https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl
The correct answer is: Use AWS Inspector API's in the pipeline for the EC2 Instances Submit your Feedback/Queries to our Experts

NEW QUESTION 100
You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?
Please select:

A. Enable server access logging for the bucket
B. Enable Cloudwatch metrics for the bucket
C. Enable Cloudwatch logs for the bucket
D. Enable AWS Config for the S3 bucket

Answer: A

Explanation:
The AWS Documentation mentions the foil
To track requests for access to your bucket you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any.
Options B and C are incorrect Cloudwatch is used for metrics and logging and cannot be used to track access requests.
Option D is incorrect since this can be used for Configuration management but for not for tracking S3 bucket requests.
For more information on S3 server logs, please refer to below UF https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLoes.html
The correct answer is: Enable server access logging for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 103
Your company has just started using AWS and created an AWS account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers fro the options given below
Please select:

A. Delete the root access account
B. Create an Admin 1AM user with the necessary permissions
C. Change the password for the root account.
D. Delete the root access keys

Answer: BD

Explanation:
The AWS Documentation mentions the following
All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account. Because you cant restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (1AM) user credentials for everyday interaction with AWS. Option A is incorrect since you cannot delete the root access account
Option C is partially correct but cannot be used as the ideal solution for safeguarding the account For more information on root access vs admin 1AM users, please refer to below URL: https://docs.aws.amazon.com/eeneral/latest/er/root-vs-iam.html
The correct answers are: Create an Admin 1AM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

NEW QUESTION 105
DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich." Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below
Please select:

A. The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the internet.

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

Answer: D

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

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

NEW QUESTION 110
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 111
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 113
A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS. What could be the strategy to adopt for managing the accounts. Please select:

A. Use multiple VPCs in the account each VPC for each department
B. Use multiple 1AM groups, each group for each department
C. Use multiple 1AM roles, each group for each department
D. Use multiple AWS accounts, each account for each department

Answer: D

Explanation:
A recommendation for this is given in the AWS Security best practices

Option A is incorrect since this would be applicable for resources in a VPC Options B and C are incorrect since operationally it would be difficult to manage For more information on AWS Security best practices please refer to the below URL
https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl
The correct answer is: Use multiple AWS accounts, each account for each department Submit your Feedback/Queries to our Experts

NEW QUESTION 116
An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below
Please select:

A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.<
B. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance call.
C. Modify the 1AM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
D. Modify the 1AM policy on the user to require MFA before deleting EC2 instances

Answer: AB

Explanation:
Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define
Options C&D are incorrect because it will not ensure that the employee cannot terminate the instance.
For more information on tagging answer resources please refer to the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins_Tags.htmll
The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance
Submit your Feedback/Queries to our Experts

NEW QUESTION 119

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

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

Answer: C

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

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

NEW QUESTION 123
A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion. What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below Please select:

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

Answer: AC

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

NEW QUESTION 127
You are planning to use AWS Configto check the configuration of the resources in your AWS account. You are planning on using an existing 1AM role and using it for the AWS Config resource. Which of the following is required to ensure the AWS config service can work as required?
Please select:

A. Ensure that there is a trust policy in place for the AWS Config service within the role
B. Ensure that there is a grant policy in place for the AWS Config service within the role
C. Ensure that there is a user policy in place for the AWS Config service within the role
D. Ensure that there is a group policy in place for the AWS Config service within the role

Answer: A

Explanation:

Options B,C and D are invalid because you need to ensure a trust policy is in place and not a grant, user or group policy or more information on the 1AM role permissions please visit the below Link: https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.htmll
The correct answer is: Ensure that there is a trust policy in place for the AWS Config service within the role
Submit your Feedback/Queries to our Experts

NEW QUESTION 128
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.

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 133
Your IT Security team has identified a number of vulnerabilities across critical EC2 Instances in the company's AWS Account. Which would be the easiest way to ensure these vulnerabilities are remediated?

Please select:

A. Create AWS Lambda functions to download the updates and patch the servers.
B. Use AWS CLI commands to download the updates and patch the servers.
C. Use AWS inspector to patch the servers
D. Use AWS Systems Manager to patch the servers

Answer: D

Explanation:
The AWS Documentation mentions the following
You can quickly remediate patch and association compliance issues by using Systems Manager Run Command. You can tat either instance IDs or Amazon EC2 tags and execute the AWSRefreshAssociation document or the AWS-RunPatchBaseline document. If refreshing the association
or re-running the patch baseline fails to resolve the compliance issue, then you need to investigate your associations, patch baselines, or instance configurations to understand why the Run Command executions did not resolve the problem
Options A and B are invalid because even though this is possible, still from a maintenance perspective it would be difficult to maintain the Lambda functions
Option C is invalid because this service cannot be used to patch servers
For more information on using Systems Manager for compliance remediation please visit the below Link:
https://docs.aws.amazon.com/systems-manaeer/latest/usereuide/sysman-compliance-fixing.html The correct answer is: Use AWS Systems Manager to patch the servers Submit your Feedback/Queries to our Experts

NEW QUESTION 137
An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of 1AM users should only access the test instances and not the production ones. How can the organization set that as a part of the policy?
Please select:

A. Launch the test and production instances in separate regions and allow region wise access to the group
B. Define the 1AM policy which allows access based on the instance ID
C. Create an 1AM policy with a condition which allows access to only small instances
D. Define the tags on the test and production servers and add a condition to the 1AM policy which allows access to specification tags

Answer: D

Explanation:
Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it
Option A is invalid because this is not a recommended practices
Option B is invalid because this is an overhead to maintain this in policies Option C is invalid because the instance type will not resolve the requirement For information on resource tagging, please visit the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usine_Tags.htmll
The correct answer is: Define the tags on the test and production servers and add a condition to the 1AM policy which allows access to specific tags
Submit your Feedback/Queries to our Experts

NEW QUESTION 138
You are creating a Lambda function which will be triggered by a Cloudwatch Event. The data from these events needs to be stored in a DynamoDB table. How should the Lambda function be given access to the DynamoDB table?
Please select:

A. Put the AWS Access keys in the Lambda function since the Lambda function by default is secure
B. Use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function.
C. Use the AWS Access keys which has access to DynamoDB and then place it in an S3 bucket.
D. Create a VPC endpoint for the DynamoDB tabl
E. Access the VPC endpoint from the Lambda function.

Answer: B

Explanation:
AWS Lambda functions uses roles to interact with other AWS services. So use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function.
Options A and C are all invalid because you should never use AWS keys for access. Option D is invalid because the VPC endpoint is used for VPCs
For more information on Lambda function Permission model, please visit the URL https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function. Submit your Feedback/Queries to our Experts

NEW QUESTION 140
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 142
A company has a requirement to create a DynamoDB table. The company's software architect has provided the following CLI command for the DynamoDB table

Which of the following has been taken of from a security perspective from the above command? Please select:

A. Since the ID is hashed, it ensures security of the underlying table.
B. The above command ensures data encryption at rest for the Customer table
C. The above command ensures data encryption in transit for the Customer table
D. The right throughput has been specified from a security perspective

Answer: B

Explanation:
The above command with the "-sse-specification Enabled=true" parameter ensures that the data for the DynamoDB table is encrypted at rest.
Options A,C and D are all invalid because this command is specifically used to ensure data encryption at rest
For more information on DynamoDB encryption, please visit the URL:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/encryption.tutorial.html The correct answer is: The above command ensures data encryption at rest for the Customer table

NEW QUESTION 147
What is the result of the following bucket policy?

Choose the correct answer
Please select:

A. It will allow all access to the bucket mybucket
B. It will allow the user mark from AWS account number 111111111 all access to the bucket but deny everyone else all access to the bucket
C. It will deny all access to the bucket mybucket
D. None of these

Answer: C

Explanation:
The policy consists of 2 statements, one is the allow for the user mark to the bucket and the next is the deny policy for all other users. The deny permission will override the allow and hence all users
will not have access to the bucket.

Options A,B and D are all invalid because this policy is used to deny all access to the bucket mybucket For examples on S3 bucket policies, please refer to the below Link: http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.htmll
The correct answer is: It will deny all access to the bucket mybucket Submit your FeedbacK/Quenes to our Experts

NEW QUESTION 152
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 Instance.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 155
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 158
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 162
You have an S3 bucket defined in AWS. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this.
Please select:

A. Enable server side encryption for the S3 bucke
B. This request will ensure that the data is encrypted first.
C. Use the AWS Encryption CLI to encrypt the data first
D. Use a Lambda function to encrypt the data before sending it to the S3 bucket.
E. Enable client encryption for the bucket

Answer: B

Explanation:
One can use the AWS Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL: https://aws.amazonxom/blogs/securirv/how4o-encrvpt-and-decrypt-your-data-with-the-awsencryption- cl
The correct answer is: Use the AWS Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

NEW QUESTION 163
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: Ihttpsy/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 165
A company's AWS account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?
Please select:

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

Answer: B

Explanation:
Option A is incorrect since you don't add a user to the 1AM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach
An 1AM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group
For more information on 1AM Groups, just browse to the below URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the 1AM groups and add users, based upon their role, to different groups and apply the policy to group
Submit your Feedback/Queries to our Experts

NEW QUESTION 168
Your CTO is very worried about the security of your AWS account. How best can you prevent hackers from completely hijacking your account?
Please select:

A. Use short but complex password on the root account and any administrators.
B. Use AWS 1AM Geo-Lock and disallow anyone from logging in except for in your city.
C. Use MFA on all users and accounts, especially on the root account.
D. Don't write down or remember the root account password after creating the AWS accoun

Answer: C

Explanation:
Multi-factor authentication can add one more layer of security to your AWS account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account

Option A is invalid because you need to have a good password policy Option B is invalid because there is no 1AM Geo-Lock Option D is invalid because this is not a recommended practices For more information on MFA, please visit the below URL http://docs.aws.amazon.com/IAM/latest/UserGuide/id credentials mfa.htmll
The correct answer is: Use MFA on all users and accounts, especially on the root account. Submit your Feedback/Queries to our Experts

NEW QUESTION 173
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 176
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.html
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 179
You work at a company that makes use of AWS resources. One of the key security policies is to ensure that all data i encrypted both at rest and in transit. Which of the following is one of the right ways to implement this.
Please select:

A. Use S3 SSE and use SSL for data in transit
B. SSL termination on the ELB
C. Enabling Proxy Protocol
D. Enabling sticky sessions on your load balancer

Answer: A

Explanation:
By disabling SSL termination, you are leaving an unsecure connection from the ELB to the back end instances. Hence this means that part of the data transit is not being encrypted.
Option B is incorrect because this would not guarantee complete encryption of data in transit Option C and D are incorrect because these would not guarantee encryption
For more information on SSL Listeners for your load balancer, please visit the below URL: http://docs.aws.amazon.com/elasticloadbalancine/latest/classic/elb-https-load-balancers.htmll The correct answer is: Use S3 SSE and use SSL for data in transit
Submit your Feedback/Queries to our Experts

NEW QUESTION 184
......

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