Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

NEW QUESTION 1
Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

A. Stream the log files to a separate Cloudtrail trail
B. Stream the log files to a separate Cloudwatch Log group
C. Create an 1AM policy that gives the desired level of access to the Cloudtrail trail
D. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group

Answer: BD

Explanation:
You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an 1AM policy.
Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement
For more information on Log Groups and Log Streams, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Workinj
For more information on Access to Cloudwatch logs, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group
Submit your Feedback/Queries to our Experts

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

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

Answer: D

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

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

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

Answer: D

Explanation:
The AWS Documentation states the following
• AWS managed CM Ks: You cannot manage key rotation for AWS managed CMKs. AWS KMS automatically rotates AWS managed keys every three years (1095 days).
Note: AWS-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365- days from when rotation is enabled.
Option A, B, C are invalid because the dettings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL
https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html
AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. This CMK is unique to your AWS account and region. Only the service that created the AWS managed CMK can use it
You can login to you 1AM dashbaord . Click on "Encryption Keys" You will find the list based on the services you are using as follows:
• aws/elasticfilesystem 1 aws/lightsail
• aws/s3

• aws/rds and many more Detailed Guide: KMS

You can recognize AWS managed CMKs because their aliases have the format aws/service-name, such as aws/redshift. Typically, a service creates its AWS managed CMK in your account when you set up the service or the first time you use the CMfC

The AWS services that integrate with AWS KMS can use it in many different ways. Some services create AWS managed CMKs in your account. Other services require that you specify a customer managed CMK that you have created. And, others support both types of CMKs to allow you the ease of an AWS managed CMK or the control of a customer-managed CMK

Rotation period for CMKs is as follows:

• AWS managed CMKs: 1095 days
• Customer managed CMKs: 365 days

Since question mentions about "CMK where backing keys is managed by AWS", its Amazon(AWS) managed and its rotation period turns out to be 1095 days{every 3 years}

For more details, please check below AWS Docs: https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html The correct answer is: After 3 years
Submit your Feedback/Queries to our Experts

NEW QUESTION 4

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

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

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

Answer: C

Explanation:

When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket

Option A is invalid because the right permissions are already provided as per the question requirement

Option B is invalid because it is not necessary that the policy has the same name as the bucket Option D is invalid because this should be the default flow for applying the policy

For more information on bucket policies please visit the below URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.htmll

The correct answer is: Change the Resource section to "arn:aws:s3:::appbucket/" Submit your Feedback/Queries to our Experts

NEW QUESTION 5

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

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

Answer: B

Explanation:

The AWS Documentation mentions the following

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects. Option A is invalid because this can be used to prevent accidental deletion of objects

Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL: https://docs.aws.ama2on.com/AmazonS3/latest/dev/ShareObiectPreSisnedURL.html

The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 6

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?
Please select:

A. Use AWS Inspector to inspect all the security Groups
B. Use the AWS Trusted Advisor to see which security groups have compromised access.
C. Use AWS Config to see which security groups have compromised access.
D. Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted accessd

Answer: B

Explanation:

The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-ofservice attacks, loss of data).
If you go to AWS Trusted Advisor, you can see the details

Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.
Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option Dis partially valid but would just be a maintenance overhead

For more information on the AWS Trusted Advisor, please visit the below URL: https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices;

The correct answer is: Use the AWS Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 7

A company is using CloudTrail to log all AWS API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.

What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below

Please select:

A. Create an S3 bucket in a dedicated log account and grant the other accounts write only acces

B. Deliver all log files from every account to this S3 bucket.

C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check

D. Run the function every 10 minutes.

E. Enable CloudTrail log file integrity validation

F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.

G. Create a Security Group that blocks all traffic except calls from the CloudTrail servic

H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:

The AWS Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log fill integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.

Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-loe-file-validationintro. htmll

For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multipleaccounts. html

The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation

Submit your Feedback/Queries to our Experts

NEW QUESTION 8

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

Please select:

A. Enable SSL certificates for the Cloudtrail logs

B. There is no need to do anything since the logs will already be encrypted

C. Enable Server side encryption for the trail

D. Enable Server side encryption for the destination S3 bucket

Answer: B

Explanation:

The AWS Documentation mentions the following.

By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about lo file delivery and validation, you can set up Amazon SNS notifications.

Option A.C and D are not valid since logs will already be encrypted

For more information on how Cloudtrail works, please visit the following URL: https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/how-cloudtrail-works.htmll

The correct answer is: There is no need to do anything since the logs will already be encrypted Submit your Feedback/Queries to our Experts

NEW QUESTION 9

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

Please select:

A. Delete the AWS keys for the root account

B. Create 1AM Groups

C. Create 1AM Roles

D. Restrict access using 1AM policies

Answer: A

Explanation:

The first level or measure that should be taken is to delete the keys for the 1AM root user

When you log into your account and go to your Security Access dashboard, this is the first step that can be seen

Option B and C are wrong because creation of 1AM groups and roles will not change the impact of leakage of AWS root access keys

Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL: https://docs.aws.amazon.com/eeneral/latest/gr/aws-access-keys-best-practices.html

The correct answer is: Delete the AWS keys for the root account Submit your Feedback/Queries to our Experts

NEW QUESTION 10
You have setup a set of applications across 2 VPC's. You have also setup VPC Peering. The applications are still not able to communicate across the Peering connection. Which network troubleshooting steps should be taken to resolve the issue?
Please select:

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

Answer: D

Explanation:
After the VPC peering connection is established, you need to ensure that the route tables are modified to ensure traffic can between the VPCs
Option A ,B and C are invalid because allowing access the Internet gateway and usage of public subnets can help for Inter, access, but not for VPC Peering.
For more information on VPC peering routing, please visit the below URL:
.com/AmazonVPC/latest/Peeri
The correct answer is: Check the Route tables for the VPCs Submit your Feedback/Queries to our Experts

NEW QUESTION 10
You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can
help in this regard?
Please select:

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

Answer: C

Explanation:
Below is a snapshot of the service limits that the Trusted Advisor can monitor

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

NEW QUESTION 14
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 15
A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.
Please select:

A. Enable CloudTrail logging in all accounts into S3 buckets
B. Enable CloudTrail logging in all accounts into Amazon Glacier
C. Ensure a lifecycle policy is defined on the S3 bucket to move the data to EBS volumes after 6 months.
D. Ensure a lifecycle policy is defined on the S3 bucket to move the data to Amazon Glacier after 6 months.

Answer: AD

Explanation:
Cloudtrail publishes the trail of API logs to an S3 bucket
Option B is invalid because you cannot put the logs into Glacier from CloudTrail
Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes For more information on Cloudtrail logging, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/cloudtrail-find-log-files.htmll
You can then use Lifecycle policies to transfer data to Amazon Glacier after 6 months For more information on S3 lifecycle policies, please visit the below URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html
The correct answers are: Enable CloudTrail logging in all accounts into S3 buckets. Ensure a lifecycle policy is defined on the bucket to move the data to Amazon Glacier after 6 months.
Submit your Feedback/Queries to our Experts

NEW QUESTION 16
You want to launch an EC2 Instance with your own key pair in AWS. How can you achieve this?
Choose 3 answers from the options given below. Please select:

A. Use a third party tool to create the Key pair
B. Create a new key pair using the AWS CLI
C. Import the public key into EC2
D. Import the private key into EC2

Answer: ABC

Explanation:
This is given in the AWS Documentation Creating a Key Pair
You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2.
Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2.
Option B is Correct, because you can use the AWS CLI to create a new key pair 1 https://docs.aws.amazon.com/cli/latest/userguide/cli-ec2-keypairs.html
Option D is invalid because the public key needs to be stored in the EC2 Instance For more information on EC2 Key pairs, please visit the below URL:
* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs
The correct answers are: Use a third party tool to create the Key pair. Create a new key pair using the AWS CLI, Import the public key into EC2
Submit your Feedback/Queries to our Experts

NEW QUESTION 20
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 24
You are building a large-scale confidential documentation web server on AWSand all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below
Please select:

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

Answer: B

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

Submit your Feedback/Queries to our Experts

NEW QUESTION 27
How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance. How can this be achieved?
Please select:

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

Answer: B

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

NEW QUESTION 32
You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3. Which of the following can be used for this purpose.
Please select:

A. AWS KMS
B. AWS Customer Keys
C. AWS managed keys
D. AWS Cloud HSM

Answer: AD

Explanation:
AWS Key Management Service (KMS) now uses FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints, which provide independent assurances about the confidentiality and integrity of your keys.
All master keys in AWS KMS regardless of their creation date or origin are automatically protected using FIPS 140-2 validated
HSMs. defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.
• FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must
be "production-grade" anc various egregious kinds of insecurity must be absent
• FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
• FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
• FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.
AWSCloudHSM provides you with a FIPS 140-2 Level 3 validated single-tenant HSM cluster in your Amazon Virtual Private Cloud (VPQ to store and use your keys. You have exclusive control over how your keys are used via an authentication mechanism independent from AWS. You interact with keys in your AWS CloudHSM cluster similar to the way you interact with your applications running in Amazon EC2.
AWS KMS allows you to create and control the encryption keys used by your applications and supported AWS services in multiple regions around the world from a single console. The service uses a FIPS 140-2 validated HSM to protect the security of your keys. Centralized management of all your keys in AWS KMS lets you enforce who can use your keys under which conditions, when they get rotated, and who can manage them.
AWS KMS HSMs are validated at level 2 overall and at level 3 in the following areas:
• Cryptographic Module Specification
• Roles, Services, and Authentication
• Physical Security
• Design Assurance
So I think that we can have 2 answers for this question. Both A & D.
• https://aws.amazon.com/blo15s/security/aws-key-management-service- now-ffers-flps-140-2- validated-cryptographic-m< enabling-easier-adoption-of-the-service-for-regulated-workloads/
• https://a ws.amazon.com/cloudhsm/faqs/
• https://aws.amazon.com/kms/faqs/
• https://en.wikipedia.org/wiki/RPS
The AWS Documentation mentions the following
AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the filexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java
Cryptography Extensions ()CE). and Microsoft CryptoNG (CNG) libraries. CloudHSM is also standardscompliant and enables you to export all of your keys to most other commercially-available HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.
All other options are invalid since AWS Cloud HSM is the prime service that offers FIPS 140-2 Level 3 compliance
For more information on CloudHSM, please visit the following url https://aws.amazon.com/cloudhsm;
The correct answers are: AWS KMS, AWS Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 33
You need to inspect the running processes on an EC2 Instance that may have a security issue. How can you achieve this in the easiest possible. Also you need to ensure that the process does not interfere with the continuous running of the instance.

Please select:

A. Use AWS Cloudtrail to record the processes running on the server to an S3 bucket.
B. Use AWS Cloudwatch to record the processes running on the server
C. Use the SSM Run command to send the list of running processes information to an S3 bucket.
D. Use AWS Config to see the changed process information on the server

Answer: C

Explanation:
The SSM Run command can be used to send OS specific commands to an Instance. Here you can check and see the running processes on an instance and then send the output to an S3 bucket. Option A is invalid because this is used to record API activity and cannot be used to record running processes.
Option B is invalid because Cloudwatch is a logging and metric service and cannot be used to record running processes.
Option D is invalid because AWS Config is a configuration service and cannot be used to record running processes.
For more information on the Systems Manager Run command, please visit the following URL: https://docs.aws.amazon.com/systems-manaEer/latest/usereuide/execute-remote-commands.htmll The correct answer is: Use the SSM Run command to send the list of running processes information to an S3 bucket. Submit your Feedback/Queries to our Experts

NEW QUESTION 37
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 40
You need to ensure that the cloudtrail logs which are being delivered in your AWS account is encrypted. How can this be achieved in the easiest way possible?
Please select:

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

Answer: A

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

NEW QUESTION 45
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 48
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 50
Your application currently uses customer keys which are generated via AWS KMS in the US east region. You now want to use the same set of keys from the EU-Central region. How can this be accomplished?
Please select:

A. Export the key from the US east region and import them into the EU-Central region
B. Use key rotation and rotate the existing keys to the EU-Central region
C. Use the backing key from the US east region and use it in the EU-Central region
D. This is not possible since keys from KMS are region specific

Answer: D

Explanation:
Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys
Option C is invalid because the backing key cannot be used to export keys This is mentioned in the AWS documentation
What geographic region are my keys stored in?
Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region
For more information on KMS please visit the following URL: https://aws.amazon.com/kms/faqs/
The correct answer is: This is not possible since keys from KMS are region specific Submit your Feedback/Queries to our Experts

NEW QUESTION 53
Your company has created a set of keys using the AWS KMS service. They need to ensure that each key is only used for certain services. For example , they want one key to be used only for the S3 service. How can this be achieved?
Please select:

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

Answer: C

Explanation:
Option A and B are invalid because mapping keys to services cannot be done via either the 1AM or bucket policy

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

NEW QUESTION 58
You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet. This instance needs to connect to an EC2 Instance that will host an Oracle database. Which of the following steps should be followed to ensure a secure setup is in place? Select 2 answers.
Please select:

A. Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication
B. Place the EC2 Instance with the Oracle database in a separate private subnet
C. Create a database security group and ensure the web security group to allowed incoming access
D. Ensure the database security group allows incoming traffic from 0.0.0.0/0

Answer: BC

Explanation:
The best secure option is to place the database in a private subnet. The below diagram from the AWS Documentation shows this setup. Also ensure that access is not allowed from all sources but just from the web servers.

Option A is invalid because databases should not be placed in the public subnet
Option D is invalid because the database security group should not allow traffic from the internet For more information on this type of setup, please refer to the below URL: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC Scenario2.
The correct answers are: Place the EC2 Instance with the Oracle database in a separate private subnet Create a database security group and ensure the web security group to allowed incoming access
Submit your Feedback/Queries to our Experts

NEW QUESTION 60
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 61
You have a bucket and a VPC defined in AWS. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?
Please select:

A. Modify the security groups for the VPC to allow access to the 53 bucket
B. Modify the route tables to allow access for the VPC endpoint
C. Modify the 1AM Policy for the bucket to allow access for the VPC endpoint
D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

Answer: D

Explanation:
This is mentioned in the AWS Documentation Restricting Access to a Specific VPC Endpoint
The following is an example of an S3 bucket policy that restricts access to a specific bucket,
examplebucket only from the VPC endpoint with the ID vpce-la2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to the specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucke via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.

Option C is incorrect because it is the bucket policy that needs to be changed and not the 1AM policy. For more information on example bucket policies for VPC endpoints, please refer to below URL: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html

The correct answer is: Modify the bucket Policy for the bucket to allow access for the VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 66
In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement
Please select:

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

Answer: B

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

NEW QUESTION 68
Which of the following is the responsibility of the customer? Choose 2 answers from the options given below.
Please select:

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

Answer: BC

Explanation:
Below is the snapshot of the Shared Responsibility Model

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

NEW QUESTION 72
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 73
Your team is designing a web application. The users for this web application would need to sign in via an external ID provider such asfacebook or Google. Which of the following AWS service would you use for authentication?
Please select:

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

Answer: A

Explanation:
The AWS Documentation mentions the following
Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users ca sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.
Option B is incorrect since this is used for identity federation

Option C is incorrect since this is pure Identity and Access management Option D is incorrect since AWS is a configuration service
For more information on AWS Cognito please refer to the below Link: https://docs.aws.amazon.com/coenito/latest/developerguide/what-is-amazon-cognito.html
The correct answer is: AWS Cognito
Submit your Feedback/Queries to our Experts

NEW QUESTION 76
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 77
You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets. Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below
Please select:

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

Answer: BD

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

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

NEW QUESTION 78
A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events. How can this be achieved? Choose 2 answers from the options given below
Please select:

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

Answer: BC

Explanation:
The AWS Documentation mentions the following
You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket
Options A and D are invalid because you have to create a trail and not a log group
For more information on managing events with cloudtrail, please visit the following URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/loHEing-manasement-and-dataevents- with-cloudtrai
The correct answers are: Create one trail that logs data events to an S3 bucket. Create another trail that logs management events to another S3 bucket
Submit your Feedback/Queries to our Experts

NEW QUESTION 82
Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below
Please select:

A. Create an 1AM user in the company account
B. Create an 1AM Role in the company account
C. Ensure the 1AM user has access for read-only to the S3 buckets
D. Ensure the 1AM Role has access for read-only to the S3 buckets

Answer: BD

Explanation:
The AWS Documentation mentions the following
To share log files between multiple AWS accounts, you must perform the following general steps. These steps are explained in detail later in this section.
Create an 1AM role for each account that you want to share log files with.
For each of these 1AM roles, create an access policy that grants read-only access to the account you want to share the log files with.
Have an 1AM user in each account programmatically assume the appropriate role and retrieve the log files.
Options A and C are invalid because creating an 1AM user and then sharing the 1AM user credentials with the vendor is a direct 'NO' practise from a security perspective.
For more information on sharing cloudtrail logs files, please visit the following URL https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-sharine-loes.htmll
The correct answers are: Create an 1AM Role in the company account Ensure the 1AM Role has access for read-only to the S3 buckets
Submit your Feedback/Queries to our Experts

NEW QUESTION 85
Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the following
Whether any ports are left open other than admin ones like SSH and RDP
Whether any ports to the database server other than ones from the web server security group are
open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?
Please select:

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

Answer: B

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

NEW QUESTION 86
An organization has setup multiple 1AM users. The organization wants that each 1AM user accesses the 1AM console only within the organization and not from outside. How can it achieve this? Please select:

A. Create an 1AM policy with the security group and use that security group for AWS console login
B. Create an 1AM policy with a condition which denies access when the IP address range is not from the organization
C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
D. Create an 1AM policy with VPC and allow a secure gateway between the organization and AWS Console

Answer: B

Explanation:
You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in aws.
Option A is invalid because you don't mention the security group in the 1AM policy Option C is invalid because security groups by default don't allow traffic
Option D is invalid because the 1AM policy does not have such an option For more information on 1AM policy conditions, please visit the URL:
http://docs.aws.amazon.com/IAM/latest/UserGuide/access pol examples.htm l#iam-policy-example-ec2-two-condition!
The correct answer is: Create an 1AM policy with a condition which denies access when the IP address range is not from the organization
Submit your Feedback/Queries to our Experts

NEW QUESTION 87
Your company is hosting a set of EC2 Instances in AWS. They want to have the ability to detect if any port scans occur on their AWS EC2 Instances. Which of the following can help in this regard?
Please select:

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

Answer: D

Explanation:
The AWS blogs mention the following to support the use of AWS GuardDuty
GuardDuty voraciously consumes multiple data streams, including several threat intelligence feeds, staying aware of malicious addresses, devious domains, and more importantly, learning to accurately identify malicious or unauthorized behavior in your AWS accounts. In combination with information gleaned from your VPC Flow Logs, AWS CloudTrail Event Logs, and DNS logs, th allows GuardDuty to

detect many different types of dangerous and mischievous behavior including probes for known vulnerabilities, port scans and probes, and access from unusual locations. On the AWS side, it looks for suspicious AWS account activity such as unauthorized deployments, unusual CloudTrail activity, patterns of access to AWS API functions, and attempts to exceed multiple service limits. GuardDuty will also look for compromised EC2 instances talking to malicious entities or services, data exfiltration attempts, and instances that are mining cryptocurrency.
Options A, B and C are invalid because these services cannot be used to detect port scans For more information on AWS Guard Duty, please refer to the below Link:
https://aws.amazon.com/blogs/aws/amazon-guardduty-continuous-security-monitoring-threatdetection; (
The correct answer is: Use AWS Guard Duty to monitor any malicious port scans Submit your Feedback/Queries to our Experts

NEW QUESTION 91
In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being recreated.
What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below
Please select:

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

Answer: D

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

NEW QUESTION 92
Your company has defined a set of S3 buckets in AWS. They need to monitor the S3 buckets and know the source IP address and the person who make requests to the S3 bucket. How can this be achieved?
Please select:

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

Answer: B

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

NEW QUESTION 95
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 99
You have private video content in S3 that you want to serve to subscribed users on the Internet. User
IDs, credentials, and subscriptions are stored in an Amazon RDS database. Which configuration will allow you to securely serve private content to your users?
Please select:

A. Generate pre-signed URLs for each user as they request access to protected S3 content
B. Create an 1AM user for each subscribed user and assign the GetObject permission to each 1AM user
C. Create an S3 bucket policy that limits access to your private content to only your subscribed users'credentials
D. Crpafp a Cloud Front CIriein Identity user for vnur suhsrrihprl users and assign the GptOhiprt oprmissinn to this user

Answer: A

Explanation:
All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able upload a specific object to your bucket but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials, specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the specified duration.
Option B is invalid because this would be too difficult to implement at a user level. Option C is invalid because this is not possible
Option D is invalid because this is used to serve private content via Cloudfront For more information on pre-signed urls, please refer to the Link:
http://docs.aws.amazon.com/AmazonS3/latest/dev/PresienedUrlUploadObiect.htmll
The correct answer is: Generate pre-signed URLs for each user as they request access to protected S3 content Submit your Feedback/Queries to our Experts

NEW QUESTION 102
You have a set of 100 EC2 Instances in an AWS account. You need to ensure that all of these instances are patched and kept to date. All of the instances are in a private subnet. How can you achieve this. Choose 2 answers from the options given below
Please select:

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

Answer: AB

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

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

NEW QUESTION 106
You have an EC2 instance with the following security configured:
1. ICMP inbound allowed on Security Group
2. ICMP outbound not configured on Security Group
3. ICMP inbound allowed on Network ACL
4. ICMP outbound denied on Network ACL
If Flow logs is enabled for the instance, which of the following flow records will be recorded? Choose 3 answers from the options give below
Please select:

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

Answer: ABD

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

NEW QUESTION 110
Your company looks at the gaming domain and hosts several Ec2 Instances as game servers. The servers each experience user loads in the thousands. There is a concern of DDos attacks on the EC2 Instances which could cause a huge revenue loss to the company. Which of the following can help mitigate this security concern and also ensure minimum downtime for the servers.
Please select:

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

Answer: B

Explanation:

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

NEW QUESTION 115
An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party. Which of the following would meet all of these conditions?
Please select:

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

Answer: C

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

Options A and B are invalid because you should not user 1AM users or 1AM Access keys Options D is invalid because you need to create a role for cross account access
For more information on Allowing access to external accounts, please visit the below URL:
|https://aws.amazon.com/blogs/apn/how-to-best-architect-your-aws-marketplace-saassubscription- across-multiple-aws-accounts;
The correct answer is: Create an 1AM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
Submit your Feedback/Queries to our Experts

NEW QUESTION 117
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 121
There is a requirement for a company to transfer large amounts of data between AWS and an onpremise location. There is an additional requirement for low latency and high consistency traffic to
AWS. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below
Please select:

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

Answer: A

Explanation:
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect you can establish private connectivity between AWS and your datacenter, office, or colocation environment which in many cases can reduce your network costs,
increase bandwidth throughput and provide a more consistent network experience than InternetQuestions
& Answers PDF P-140 based connections.
Options B and C are invalid because these options will not reduce network latency Options D is invalid because this is only used to connect 2 VPC's
For more information on AWS direct connect, just browse to the below URL: https://aws.amazon.com/directconnect
The correct answer is: Provision a Direct Connect connection to an AWS region using a Direct Connect partner. omit your Feedback/Queries to our Experts

NEW QUESTION 123
You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?
Please select:

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

Answer: D

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

NEW QUESTION 125
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

AWS-Certified-Security-Specialty Practice Exam Features:

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

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

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

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

100% Actual & Verified — Instant Download, Please Click
[Order The AWS-Certified-Security-Specialty Practice Test Here](https://www.certshared.com/exam/AWS-Certified-Security-Specialty/)