



Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

You are hosting a web site via website hosting on an S3 bucket - <http://demo.s3-website-us-east-1.amazonaws.com>. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages, they are getting a blocked Javascript error. How can you rectify this?
Please select:

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

Answer: A

Explanation:

Your answer is incorrect Answer-A

Such a scenario is also given in the AWS Documentation Cross-Origin Resource Sharing:

Use-case Scenarios

The following are example scenarios for using CORS:

- Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint <http://website.s3-website-us-east-1.amazonaws.com>. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com.
- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

Option B is invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects

Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects

For more information on Cross Origin Resource sharing, please visit the following URL

- <https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>

The correct answer is: Enable CORS for the bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 2

Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

- A. Create a Cloudwatch Events Rule s
- B. Create a Cloudwatch Logs Rule
- C. Use a Lambda function
- D. Use Cloudtrail API call

Answer: AC

Explanation:

Below is a snippet from the AWS blogs on a solution

Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:

<https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activity>

The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts

NEW QUESTION 3

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 IAM policy that gives the desired level of access to the Cloudtrail trail
- D. Create an IAM 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 IAM 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/Working>

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 IAM policy that gives the desired level of access to the Cloudwatch Log group

Submit your Feedback/Queries to our Experts

NEW QUESTION 4

You have an EC2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective
Please select:

- A. Use a VPC endpoint
- B. Attach an Internet gateway to the subnet
- C. Attach a VPN connection to the VPC
- D. Use VPC Peering

Answer: A

Explanation:

The AWS Documentation mentions the following

You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and AWS KMS is conducted entirely within the AWS network.

Option B is invalid because this could open threats from the internet

Option C is invalid because this is normally used for communication between on-premise environments and AWS.

Option D is invalid because this is normally used for communication between VPCs

For more information on accessing KMS via an endpoint, please visit the following URL <https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html>

The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

NEW QUESTION 5

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 VPC
- B. Configure the Lambda function to access resources in the VPC.
- C. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table
- D. Attach the policy to the DynamoDB table.
- E. Create an IAM user with permissions to write to the DynamoDB table
- F. Store an access key for that user in the Lambda environment variables.
- G. Create an IAM service role with permissions to write to the DynamoDB table
- H. Associate that role with the Lambda function.

Answer: D

Explanation:

The ideal way is to create an IAM 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 IAM role (execution role) associated with it. You specify the IAM 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 IAM 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 resource 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 IAM 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 IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

Submit your Feedback/Queries to our Experts

NEW QUESTION 6

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 IAM Roles with a timestamp to limit the access
- D. Use IAM 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.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

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

NEW QUESTION 7

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 access

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-of-service 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 D is 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 8

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

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

Answer: A

Explanation:

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

NEW QUESTION 9

Which of the following is used as a secure way to log into an EC2 Linux Instance? Please select:

- A. IAM User name and password
- B. Key pairs
- C. AWS Access keys
- D. AWS SDK keys

Answer: B

Explanation:

The AWS Documentation mentions the following
Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
Option A, C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on AWS Security credentials, please visit the below URL: <https://docs.aws.amazon.com/general/latest/en/aws-sec-cred-types.html>
The correct answer is: Key pairs
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 Internet access, but not for VPC Peering.
For more information on VPC peering routing, please visit the below URL:
<https://docs.aws.amazon.com/VPC/latest/Peering>
The correct answer is: Check the Route tables for the VPCs Submit your Feedback/Queries to our Experts

NEW QUESTION 10

A company has a legacy application that outputs all logs to a local text file. Logs from all applications running on AWS must be continually monitored for security related messages. What can be done to allow the company to deploy the legacy application on Amazon EC2 and still meet the monitoring requirement? Please select:

- A. Create a Lambda function that mounts the EBS volume with the logs and scans the logs for security incident
- B. Trigger the function every 5 minutes with a scheduled Cloudwatch event.
- C. Send the local text log files to CloudWatch Logs and configure a CloudWatch metric filter
- D. Trigger cloudwatch alarms based on the metrics.
- E. Install the Amazon inspector agent on any EC2 instance running the legacy application
- F. Generate CloudWatch alerts based on any Amazon inspector findings.
- G. Export the local text log files to CloudTrail
- H. Create a Lambda function that queries the CloudTrail logs for security incidents using Athena.

Answer: B

Explanation:

One can send the log files to Cloudwatch Logs. Log files can also be sent from On-premise servers. You can then specify metrics to search the logs for any specific values. And then create alarms based on these metrics.

Option A is invalid because this will be just a long over drawn process to achieve this requirement. Option C is invalid because AWS Inspector cannot be used to monitor for security related messages. Option D is invalid because files cannot be exported to AWS CloudTrail.

For more information on Cloudwatch logs agent please visit the below URL:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html>

The correct answer is: Send the local text log files to Cloudwatch Logs and configure a Cloudwatch metric filter. Trigger cloudwatch alarms based on the metrics. Submit your Feedback/Queries to our Experts

NEW QUESTION 13

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/developerguide/deleting-keys.html>

The correct answer is: Disable the keys. Submit your Feedback/Queries to our Experts

NEW QUESTION 15

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

Each CMK must be rotated annually.

What two methods can the security team use to rotate each key? Select 2 answers from the options given below.

Please select:

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

Answer: AD

Explanation:

The AWS Documentation mentions the following:

Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually.

Rotating Keys Manually

You might want to create a new CMK and use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.

When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the same CMK to decrypt the data.

A. As long as you keep both

the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.

Option B is invalid because you also need to point the key alias to the new key. Option C is invalid because existing CMK keys cannot be rotated as they are

Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key.

For more information on Key rotation please see the below Link: <https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

The correct answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK; Point the key alias to the new CMK.

Submit your Feedback/Queries to our Experts

NEW QUESTION 18

A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?
Please select:

- A. Access the S3 bucket through a proxy server
- B. Access the S3 bucket through a NAT gateway.
- C. Access the S3 bucket through a VPC endpoint for S3
- D. Access the S3 bucket through the SSL protected S3 endpoint

Answer: C

Explanation:

The AWS Documentation mentions the following

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Option A is invalid because using a proxy server is not sufficient enough

Option B and D are invalid because you need secure communication which should not traverse the internet

For more information on VPC endpoints please see the below link <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>

The correct answer is: Access the S3 bucket through a VPC endpoint for S3 Submit your Feedback/Queries to our Experts

NEW QUESTION 23

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](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html).

The correct answer is: Consider moving the database server to a private subnet Submit your Feedback/Queries to our Experts

NEW QUESTION 24

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

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

Answer: AE

Explanation:

Create a Direct Connect connection so that corporate users can access the AWS account

Option B is incorrect because 1AM policies are not directly mapped to group memberships in the corporate directory. It is 1AM roles which are mapped.

Option C is incorrect because Lambda functions is an incorrect option to assign roles.

Option D is incorrect because 1AM users are not directly mapped to employees' corporate identities. For more information on Direct Connect, please refer to below URL:

' <https://aws.amazon.com/directconnect/>

From the AWS Documentation, for federated access, you also need to ensure the right policy permissions are in place

Configure permissions in AWS for your federated users

The next step is to create an 1AM role that establishes a trust relationship between 1AM and your organization's IdP that identifies your IdP as a principal (trusted entity) for purposes of federation. The role also defines what users authenticated your organization's IdP are allowed to do in AWS. You can use the 1AM console to create this role. When you create the trust policy that indicates who can assume the role, you specify the SAML provider that you created earlier in 1AM along with one or more SAML attributes that a user must match to be allowed to assume the role. For example, you can

specify that only users whose SAML eduPersonOrgDN value is ExampleOrg are allowed to sign in. The role wizard automatically adds a condition to test the saml:aud attribute to make sure that the role is assumed only for sign-in to the AWS Management Console. The trust policy for the role might look like this:

For more information on SAML federation, please refer to below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable Note: What directories can I use with AWS SSO?

You can connect AWS SSO to Microsoft Active Directory, running either on-premises or in the AWS Cloud. AWS SSO supports AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, and AD Connector. AWS SSO does not support Simple AD. See AWS Directory Service

Getting Started to learn more.

To connect to your on-premises directory with AD Connector, you need the following: VPC

Set up a VPC with the following:

- At least two subnets. Each of the subnets must be in a different Availability Zone.
- The VPC must be connected to your on-premises network through a virtual private network (VPN) connection or AWS Direct Connect.

- The VPC must have default hardware tenancy.

• <https://aws.amazon.com/single-sign-on/>

• <https://aws.amazon.com/single-sign-on/faqs/>

• <https://aws.amazon.com/bloj/using-corporate-credentials/>

• <https://docs.aws.amazon.com/directoryservice/latest/admin->

The correct answers are: Create a Direct Connect connection between on-premise network and AWS. Use an AD connector connecting AWS with on-premise active directory.. Create an 1AM role that establishes a trust relationship between 1AM and corporate directory identity provider (IdP)

Submit your Feedback/Queries to our Experts

NEW QUESTION 28

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 :allow 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 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.html>

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 31

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 Amazon S3 resources.

You can enforce the MFA authentication requirement using the aws:MultiFactorAuthAge key in a bucket policy. 1AM users can 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 32

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 way 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-](https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html)

[manaEer/latest/userguide/execute-remote-commands.html](https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html) 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

You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process. Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.

Please select:

- A. Check to see if the right role has been assigned to the EC2 instances
- B. Check to see if the IAM user has the right permissions for EC2
- C. Ensure that agent is running on the instances.
- D. Check the Instance status by using the Health AP

Answer: ACD

Explanation:

For ensuring that the instances are configured properly you need to ensure the followi .

1) You installed the latest version of the SSM Agent on your instance

2) Your instance is configured with an AWS Identity and Access Management (IAM) role that enables the instance to communicate with the Systems Manager API

3) You can use the Amazon EC2 Health API to quickly determine the following information about Amazon EC2 instances The status of one or more instances

The last time the instance sent a heartbeat value The version of the SSM Agent

The operating system

The version of the EC2Config service (Windows) The status of the EC2Config service (Windows)

Option B is invalid because IAM users are not supposed to be directly granted permissions to EC2 Instances For more information on troubleshooting AWS SSM, please visit the following URL: <https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-remotecommands.html>

The correct answers are: Check to see if the right role has been assigned to the EC2 Instances, Ensure that agent is running on the Instances., Check the Instance status by using the Health API.

Submit your Feedback/Queries to our Experts

NEW QUESTION 42

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

Please select:

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

Answer: B

Explanation:

Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.

<https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html>

A is incorrect because Creating a new CMK and attaching it to the exiting volume will not allow the data to be decrypted, you cannot attach customer master keys after the volume is encrypted

Option C and D are invalid because once the key has been deleted, you cannot recover it For more information on EBS Encryption with KMS, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>

The correct answer is: You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable. Submit your Feedback/Queries to our Experts

NEW QUESTION 45

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

Please select:

- A. Search the Cloud Watch logs to find for the suspicious activity which occurred 11 days ago
- B. Search the Cloudtrail event history on the API events which occurred 11 days ago.
- C. Search the Cloud Watch metrics to find for the suspicious activity which occurred 11 days ago
- D. Use AWS Config to get the API calls which were made 11 days ag

Answer: B

Explanation:

The Cloud Trail event history allows to view events which are recorded for 90 days. So one can use a metric filter to gather the API calls from 11 days ago. Option A and C is invalid because Cloudwatch is used for logging and not for monitoring API activity Option D is invalid because AWSConfig is a configuration service and not for monitoring API activity For more information on AWS Cloudtrail, please visit the following URL:
<https://docs.aws.amazon.com/awscloudtrail/latest/useruide/how-cloudtrail-works.html>

Note:

In this question we assume that the customer has enabled cloud trail service.

AWS CloudTrail is enabled by default for ALL CUSTOMERS and will provide visibility into the past seven days of account activity without the need for you to configure a trail in the service to get started. So for an activity that happened 11 days ago to be stored in the cloud trail we need to configure the trail manually to ensure that it is stored in the events history.

- <https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-awscustomers/> The correct answer is: Search the Cloudtrail event history on the API events which occurred 11 days ago.

NEW QUESTION 50

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/useruide/encryptine-cloudtrail-loe-files-withaws-kms.html>

The correct answer is: Don't do anything since CloudTrail logs are automatically encrypted. Submit your Feedback/Queries to our Experts

NEW QUESTION 53

You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved? Please select:

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

Answer: C

Explanation:

Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket.

Option D is invalid because this is used for programmatic access to AWS resources

You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the AWS Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers) Topics

- Creating CloudFront Key Pairs for Your Trusted Signers
- Reformatting the CloudFront Private Key (.NET and Java Only)
- Adding Trusted Signers to Your Distribution
- Verifying that Trusted Signers Are Active (Optional) 1 Rotating CloudFront Key Pairs

To create signed URLs or signed cookies, you need at least one AWS account that has an active CloudFront key pair. This accou is known as a trusted signer.

The trusted signer has two purposes:

- As soon as you add the AWS account ID for your trusted signer to your distribution, CloudFront starts to require that users us signed URLs or signed cookies to access your objects.

' When you create signed URLs or signed cookies, you use the private key from the trusted signer's key pair to sign a portion of the URL or the cookie. When someone requests a restricted object CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed.

For more information on Cloudfront private trusted content please visit the following URL:

- <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contenttrusted-s>

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

NEW QUESTION 58

Your company currently has a set of EC2 Instances hosted in a VPC. The IT Security department is suspecting a possible DDos attack on the instances. What can you do to zero in on the IP addresses which are receiving a flurry of requests. Please select:

- A. Use VPC Flow logs to get the IP addresses accessing the EC2 Instances
- B. Use AWS Cloud trail to get the IP addresses accessing the EC2 Instances
- C. Use AWS Config to get the IP addresses accessing the EC2 Instances
- D. Use AWS Trusted Advisor to get the IP addresses accessing the EC2 Instances

Answer: A

Explanation:

With VPC Flow logs you can get the list of IP addresses which are hitting the Instances in your VPC. You can then use the information in the logs to see which external IP addresses are sending a flurry of requests which could be the potential threat for a DDos attack.

Option B is incorrect. CloudTrail records AWS API calls for your account. VPC Flow logs logs network traffic for VPC, subnets, network interfaces, etc.

As per AWS,

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC, whereas AWS

CloudTrail is a service that captures API calls and delivers the log files to an Amazon S3 bucket that you specify.

Option C is invalid. This is a config service and will not be able to get the IP addresses.

Option D is invalid because this is a recommendation service and will not be able to get the IP addresses.

For more information on VPC Flow Logs, please visit the following URL: <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>

The correct answer is: Use VPC Flow logs to get the IP addresses accessing the EC2 Instances. Submit your Feedback/Queries to our Experts

NEW QUESTION 63

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 IAM users.
- B. Delete all custom created IAM policies
- C. Delete the access keys for the root account
- D. Confirm MFA on a secure device
- E. Change the password for the root account
- F. Change the password for all IAM 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 on a secure device
3. Change the password for the root account

This will ensure the employee who has left has no chance 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 on a secure device. Change the password for the root account.

Submit Your Feedback/Queries to our Experts

NEW QUESTION 64

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 66

You have a requirement to conduct penetration testing on the AWS Cloud for a couple of EC2 Instances. How could you go about doing this? Choose 2 right answers from the options given below. Please select:

- A. Get prior approval from AWS for conducting the test
- B. Use a pre-approved penetration testing tool.
- C. Work with an AWS partner and no need for prior approval request from AWS
- D. Choose any of the AWS instance type

Answer: AB

Explanation:

You can use a pre-approved solution from the AWS Marketplace. But till date the AWS Documentation still mentions that you have to get prior approval before conducting a test on the AWS Cloud for EC2 Instances.

Option C and D are invalid because you have to get prior approval first. AWS Docs provides following details:

"For performing a penetration test on AWS resources first of all we need to take permission from AWS and complete a requisition form and submit it for approval.

The form should contain information about the instances you wish to test, identify the expected start and end dates/times of your test, and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days.

from the start date."

(

At this time, our policy does not permit testing small or micro RDS instance types. Testing of ml

.small, t1 .micro or t2.nano EC2 instance types is not permitted.

For more information on penetration testing please visit the following URL: <https://aws.amazon.com/security/penetration-testing/>

The correct answers are: Get prior approval from AWS for conducting the test Use a pre-approved penetration testing tool. Submit your Feedback/Queries to our Experts

NEW QUESTION 69

You currently have an S3 bucket hosted in an AWS Account. It holds information that needs to be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.

Please select:

- A. Ensure an IAM role is created which can be assumed by the partner account.
- B. Ensure an IAM user is created which can be assumed by the partner account.
- C. Ensure the partner uses an external ID when making the request
- D. Provide the ARN for the role to the partner account
- E. Provide the Account ID to the partner account
- F. Provide access keys for your account to the partner account

Answer: ACD

Explanation:

Option B is invalid because Roles are assumed and not IAM users

Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner

The below diagram from the AWS documentation showcases an example on this wherein an IAM role and external ID is used to access an AWS account resources

For more information on creating roles for external ID'S please visit the following URL:

The correct answers are: Ensure an IAM role is created which can be assumed by the partner account. Ensure the partner uses an external ID when making the request Provide the ARN for the role to the partner account

NEW QUESTION 74

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 IAM 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 IAM 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 IAM or bucket policy

Option D is invalid because keys for IAM 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:ViaService 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/developerguide/policy-conditions.html>

The correct answer is: Use the kms:ViaService condition in the Key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 78

An EC2 Instance hosts a Java based application that accesses 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 accesses the Dynamo table

Please select:

- A. Use IAM 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 IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- D. Use IAM 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 are 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 IAM Roles, please refer to the below URL:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

The correct answer is: Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 81

A company is planning to run a number of Admin related scripts using the AWS Lambda service. There is a need to understand if there are any errors encountered when the script runs. How can this be accomplished in the most effective manner.

Please select:

- A. Use Cloudwatch metrics and logs to watch for errors
- B. Use Cloudtrail to monitor for errors
- C. Use the AWS Config service to monitor for errors
- D. Use the AWS inspector service to monitor for errors

Answer: A

Explanation:

The AWS Documentation mentions the following

AWS Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function. Lambda logs all requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs.

Option B,C and D are all invalid because these services cannot be used to monitor for errors. I

For more information on Monitoring Lambda functions, please visit the following URL: <https://docs.aws.amazon.com/lambda/latest/dg/monitorine-functions-logs.html>

The correct answer is: Use Cloudwatch metrics and logs to watch for errors Submit your Feedback/Queries to our Experts

NEW QUESTION 85

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.pdf>

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 87

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](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 90

A company has set up the following structure to ensure that their S3 buckets always have logging enabled

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

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

Answer: B

Explanation:

The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes. Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.

Option D is invalid because you don't necessarily need to use the API gateway service

For more information on accessing resources from a Lambda function, please refer to below URL <https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.html>

The correct answer is: The AWS Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 91

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

Please select:

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

Answer: B

Explanation:

The AWS Documentation mentions the following

You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app.

Option A is incorrect since you need to create cognito groups and not endpoints

Options C and D are incorrect since these would be overheads when you can use AWS Cognito For more information on AWS Cognito user groups please refer to the below Link: <https://docs.aws.amazon.com/coenito/latest/developersuide/cognito-user-pools-user-groups.html> The correct answer is: Create different cognito groups, one for the readers and the other for the contributors. Submit your Feedback/Queries to our Experts

NEW QUESTION 96

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.com/2016/11/21/waf-sandwich/>

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 101

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.html

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 104

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below
Please select:

- A. Determine the age of the master key
- B. See who is assigned permissions to the master key
- C. See Cloudtrail for usage of the key
- D. Use AWS CloudWatch events for events generated for the key

Answer: BC

Explanation:

The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs

Option A is invalid because seeing how long ago the key was created would not determine the usage of the key

Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation

Examining CMK Permissions to Determine the Scope of Potential Usage

Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key.

Examining AWS CloudTrail Logs to Determine Actual Usage

AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is

located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it

For more information on determining the usage of CMK keys, please visit the following URL: <https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html>

The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key Submit your Feedback/Queries to our Experts

NEW QUESTION 105

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 IAM user in the company account
- B. Create an IAM Role in the company account
- C. Ensure the IAM user has access for read-only to the S3 buckets
- D. Ensure the IAM 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 IAM role for each account that you want to share log files with.

For each of these IAM roles, create an access policy that grants read-only access to the account you want to share the log files with.

Have an IAM user in each account programmatically assume the appropriate role and retrieve the log files.

Options A and C are invalid because creating an IAM user and then sharing the IAM 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-share-logs.html>

The correct answers are: Create an IAM Role in the company account Ensure the IAM Role has access for read-only to the S3 buckets

Submit your Feedback/Queries to our Experts

NEW QUESTION 108

An application is designed to run on an EC2 Instance. The application 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 IAM user to the application that has specific access to only that S3 bucket
- C. Assign an IAM Role and assign it to the EC2 Instance
- D. Assign an IAM group and assign it to the EC2 Instance

Answer: C

Explanation:

The below diagram from the AWS whitepaper shows the best security practise 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.pdf

The correct answer is: Assign an IAM Role and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 111

Your company has an EC2 Instance hosted in AWS. This EC2 Instance hosts an application. Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring? Which one of the below steps can help address this issue? Please select:

- A. Use the VPC Flow Logs.
- B. Use a network monitoring tool provided by an AWS partner.
- C. Use another instance
- D. Setup a port to "promiscuous mode" and sniff the traffic to analyze the packet
- E. -
- F. Use Cloudwatch metric

Answer: B

NEW QUESTION 115

You are planning to use AWS Config to check the configuration of the resources in your AWS account. You are planning on using an existing IAM 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 IAM role permissions please visit the below Link: <https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.html>

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 118

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 in the AWS Documentation 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 IAM 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 119

An organization has launched 5 instances: 2 for production and 3 for testing. The organization wants that one particular group of IAM 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 IAM policy which allows access based on the instance ID
- C. Create an IAM 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 IAM 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 practice

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/Using_Tags.html

The correct answer is: Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags

Submit your Feedback/Queries to our Experts

NEW QUESTION 124

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

- A. Create an IAM policy with the security group and use that security group for AWS console login
- B. Create an IAM 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> [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 128

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 133

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

Please select:

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

Answer: C

Explanation:

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

Options A,B and D are invalid because Cloudfront is specifically used to protect sites against DDoS attacks For more information on security with Cloudfront, please refer to the below Link: [https://d1.awsstatic.com/whitepapers/Security/Secure content delivery with CloudFront whitepaper.pdf](https://d1.awsstatic.com/whitepapers/Security/Secure_content_delivery_with_CloudFront_whitepaper.pdf)

The correct answer is: DDoS attacks

Submit your Feedback/Queries to our Experts

NEW QUESTION 134

Your company has many AWS accounts defined and all are managed via AWS Organizations. One AWS account has a S3 bucket that has critical dat

- A. How can we ensure that all the users in the AWS organisation have access to this bucket? Please select:
- B. Ensure the bucket policy has a condition which involves aws:PrincipalOrgID
- C. Ensure the bucket policy has a condition which involves aws:AccountNumber
- D. Ensure the bucket policy has a condition which involves aws:PrincipalID
- E. Ensure the bucket policy has a condition which involves aws:OrgID

Answer: A

Explanation:

The AWS Documentation mentions the following

AWS Identity and Access Management (IAM) now makes it easier for you to control access to your AWS resources by using the AWS organization of IAM principals (users and roles). For some services, you grant permissions using resource-based policies to specify the accounts and principals that can access the resource and what actions they can perform on it. Now, you can use a new condition key, aws:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account in the organization

Option B.C and D are invalid because the condition in the bucket policy has to mention aws:PrincipalOrgID

For more information on controlling access via Organizations, please refer to the below Link: <https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-awsorganization-of-iam-principal/>

(

The correct answer is: Ensure the bucket policy has a condition which involves aws:PrincipalOrgID Submit your Feedback/Queries to our Experts

NEW QUESTION 136

Your team is experimenting with the API gateway service for an application. There is a need to implement a custom module which can be used for authentication/authorization for calls made to the API gateway. How can this be achieved?

Please select:

- A. Use the request parameters for authorization
- B. Use a Lambda authorizer
- C. Use the gateway authorizer
- D. Use CORS on the API gateway

Answer: B

Explanation:

The AWS Documentation mentions the following

An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.

Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway

For more information on using the API gateway Lambda authorizer please visit the URL:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambdaauthorizer.html>

The correct answer is: Use a Lambda authorizer Submit your Feedback/Queries to our Experts

NEW QUESTION 137

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 IAM user for each subscribed user and assign the GetObject permission to each IAM user
- C. Create an S3 bucket policy that limits access to your private content to only your subscribed users'credentials
- D. Create a CloudFront Origin Identity user for your subscribers and assign the GetObject permission 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/PresignedUrlUploadObject.html>

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 138

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 Link: <https://aws.amazon.com/blogs/security/how-to-patch-linux-workloads-on-aws/>

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 140

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 bucket
- 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.amazon.com/blogs/security/how-to-encrypt-and-decrypt-your-data-with-the-aws-encryption-cli/>

The correct answer is: Use the AWS Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

NEW QUESTION 142

Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.

Please select:

A.

B.

C.

D.

A.

Answer: A

Explanation:

The condition of "s3:x-amz-server-side-encryption":"aws:kms" ensures that objects uploaded need to be encrypted.

Options B,C and D are invalid because you have to ensure the condition of "s3:x-amz-server-side-encryption":"aws:kms" is present

For more information on AWS KMS best practices, just browse to the below URL:

<https://dl.awsstatic.com/whitepapers/aws-kms-best-practices.pdf>

Submit your Feedback/Queries to our Expert

NEW QUESTION 144

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 IAM 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 IAM 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 IAM 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 146

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

Please select:

A. A Bastion host should be on a private subnet and never a public subnet due to security concerns

B. A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network

C. Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.

D. A Bastion host should maintain extremely tight security and monitoring as it is available to the public

Answer: C

Explanation:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

In AWS, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and

then use that session to manage other hosts in the private subnets.

Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring For more information on bastion hosts, just browse to the below URL:

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.

Submit your Feedback/Queries to our Experts

NEW QUESTION 149

Your company uses AWS to host its resources. They have the following requirements

- 1) Record all API calls and Transitions
 - 2) Help in understanding what resources are there in the account
 - 3) Facility to allow auditing credentials and logins
- Which services would suffice the above requirements
Please select:

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

Answer: C

Explanation:

You can use AWS CloudTrail to get a history of AWS API calls and related events for your account. This history includes calls made with the AWS Management Console, AWS Command Line Interface, AWS SDKs, and other AWS services.

Options A,B and D are invalid because you need to ensure that you use the services of CloudTrail, AWS Config, IAM Credential Reports

For more information on Cloudtrail, please visit the below URL: <http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

AWS Config is a service that enables you to assess, audit and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management and operational troubleshooting.

For more information on the config service, please visit the below URL <https://aws.amazon.com/config/>

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the AWS Management Console, the AWS SDKs and Command Line Tools, or the IAM API.

For more information on Credentials Report, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

The correct answer is: CloudTrail, AWS Config, IAM Credential Reports Submit your Feedback/Queries to our Experts

NEW QUESTION 150

You work at a company that makes use of AWS resources. One of the key security policies is to ensure that all data is 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/elasticloadbalancing/latest/classic/elb-https-load-balancers.html> The correct answer is: Use S3 SSE and use SSL for data in transit

Submit your Feedback/Queries to our Experts

NEW QUESTION 155

There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's.

Please select:

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

Answer: B

Explanation:

NACL acts as a firewall at the subnet level of the VPC and we can deny the offending IP address block

at the subnet level using NACL rules to block the incoming traffic to the VPC instances. Since NACL rules are applied as per the Rule numbers make sure that this rule number should take precedence over other rule numbers if there are any such rules that will allow traffic from these IP ranges. The lowest rule number has more precedence over a rule that has a higher number.

The AWS Documentation mentions the following as a best practices for IAM users

For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone). Options C is invalid because these options are not available

Option D is invalid because there is not root access for users

For more information on IAM best practices, please visit the below URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

The correct answer is: Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.

omit your Feedback/Queries to our Experts

NEW QUESTION 156

.....

Relate Links

100% Pass Your AWS-Certified-Security-Specialty Exam with Examible Prep Materials

<https://www.exambible.com/AWS-Certified-Security-Specialty-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>