

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

<https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/>



NEW QUESTION 1

You are designing a custom IAM policy that would allow users to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?

A.

B.

C.

D.

A.

Answer: A

Explanation:

The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated.

Option B and C are wrong since the `aws:MultiFactorAuthPresent` clause should be marked as true. Here you are saying that only if the user has been MFA activated, that means it is true, then allow access.

Option D is invalid because the `Bool` clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."

Here in this scenario the `Bool` attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.

For more information on an example on such a policy, please visit the following URL:

NEW QUESTION 2

A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?

Please select:

A. Use KMS and the normal KMS encryption keys

B. Use KMS and use an external key material

C. Use S3 Server Side encryption

D. Use Cloud HSM

Answer: D

Explanation:

The AWS Documentation mentions the following

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware

Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are design and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

Option A,B and Care invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM

For more information on CloudHSM, please visit the following URL: <https://aws.amazon.com/cloudhsm/faq>:

The correct answer is: Use Cloud HSM 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 1AM policy that gives the desired level of access to the Cloudtrail trail
- D. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group

Answer: BD

Explanation:

You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an 1AM policy.

Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement

For more information on Log Groups and Log Streams, please visit the following URL:

* <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/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 1AM policy that gives the desired level of access to the Cloudwatch Log group

Submit your Feedback/Queries to our Experts

NEW QUESTION 4

An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK. Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below

Please select:

- A. Add the EC2 instance role as a trusted service to the SSM service role.
- B. Add permission to use the KMS key to decrypt to the SSM service role.
- C. Add permission to read the SSM parameter to the EC2 instance role..
- D. Add permission to use the KMS key to decrypt to the EC2 instance role
- E. Add the SSM service role as a trusted service to the EC2 instance rol

Answer: CD

Explanation:

The below example policy from the AWS Documentation is required to be given to the EC2 Instance in order to read a secure string from AWS KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.

Option A is invalid because roles can be attached to EC2 and not EC2 roles to SSM Option B is invalid because the KMS key does not need to decrypt the SSM service role.

Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html>

The correct answers are: Add permission to read the SSM parameter to the EC2 instance role., Add permission to use the KMS key to decrypt to the EC2 instance role

Submit your Feedback/Queries to our Experts

NEW QUESTION 5

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

Please select:

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

Answer: B

Explanation:

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

If you go to AWS Trusted Advisor, you can see the details

Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.

Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option Dis partially valid but would just be a maintenance overhead

For more information on the AWS Trusted Advisor, please visit the below URL: <https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices>;
The correct answer is: Use the AWS Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 6

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

Please select:

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

Answer: C

Explanation:

This concept is given in the AWS Documentation

How do I submit a penetration testing request for my AWS resources? Issue

I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?

Resolution

Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.

AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.

If your request is approved, you'll receive an authorization number.

Option A,B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests

For more information on penetration testing, please visit the below URL

* <https://aws.amazon.com/security/penetration-testing/>

* <https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/> (

The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

NEW QUESTION 7

Your company is planning on hosting an internal network in AWS. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.

Please select:

- A. Consider using Windows Server 2016 Certificate Manager
- B. Consider using AWS Certificate Manager
- C. Consider using AWS Access keys to generate the certificates
- D. Consider using AWS Trusted Advisor for managing the certificates

Answer: B

Explanation:

The AWS Documentation mentions the following

ACM is tightly linked with AWS Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally.

Private certificates cannot be publicly trusted

Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", AWS Certificate Manager should be used Option C and D are invalid because these cannot be used for managing certificates.

For more information on ACM, please visit the below URL: <https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

The correct answer is: Consider using AWS Certificate Manager 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 OpsWor 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/eeneral/latest/gr/aws-security-audit-euide.html>

The correct answer is: Conduct an audit on a yearly basis Submit your Feedback/Queries to our Experts

NEW QUESTION 9

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

Please select:

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

Answer: C

Explanation:

Option A is invalid because the normal AWS Shield Service will not help in immediate action against a DDos attack. This can be done via the AWS Shield Advanced Service

Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDos attacks.

Option D is invalid because this is a logging service for AWS Services but cannot specifically protect against DDos attacks.

The AWS Documentation mentions the following

AWS Shield Advanced provides enhanced protections for your applications running on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated attacks. AWS Shield Advanced is available to AWS Business Support and AWS Enterprise Support customers.

AWS Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDos attacks. AWS Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDoS Response Team (DRT) 24x7 to manage and mitigate their application layer DDos attacks.

For more information on AWS Shield, please visit the below URL: <https://aws.amazon.com/shield/faqs>;

The correct answer is: Consider using the AWS Shield Advanced Service Submit your Feedback/Queries to our Experts

NEW QUESTION 10

You need to ensure that objects in an S3 bucket are available in another region. This is because of the criticality of the data that is hosted in the S3 bucket. How can you achieve this in the easiest way possible?

Please select:

- A. Enable cross region replication for the bucket
- B. Write a script to copy the objects to another bucket in the destination region
- C. Create an S3 snapshot in the destination region
- D. Enable versioning which will copy the objects to the destination region

Answer: A

Explanation:

Option B is partially correct but a big maintenance overhead to create and maintain a script when the functionality is already available in S3

Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The AWS Documentation mentions the following

Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions.

For more information on Cross region replication in the Simple Storage Service, please visit the below URL:

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

The correct answer is: Enable cross region replication for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 10

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 11

Your company makes use of S3 buckets for storing data

- A. There is a company policy that all services should have logging enabled
- B. How can you ensure that logging is always enabled for created S3 buckets in the AWS Account? Please select:
- C. Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
- D. Use AWS Config Rules to check whether logging is enabled for buckets
- E. Use AWS Cloudwatch metrics to check whether logging is enabled for buckets
- F. Use AWS Cloudwatch logs to check whether logging is enabled for buckets

Answer: B

Explanation:

This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers

Example rule with configuration change trigger

1. You add the AWS Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.

Option A is invalid because AWS Inspector cannot be used to scan all buckets

Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.

For more information on Config Rules please see the below Link: <https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

The correct answer is: Use AWS Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 13

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 16

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 20

A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below Please select:

- A. AWS VPN
- B. AWS VPC Peering
- C. AWS NAT gateways
- D. AWS Direct Connect

Answer: AD

Explanation:

The AWS Document mention the following which supports the requirement

Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the AWS Cloud. Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet For more information on VPN Connections, please visit the following url <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html>
The correct answers are: AWS VPN, AWS Direct Connect Submit your Feedback/Queries to our Experts

NEW QUESTION 22

You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-premise Active Directory. Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below. Please select:

- A. Ensure the right match is in place for On-premise AD Groups and 1AM Roles.
- B. Ensure the right match is in place for On-premise AD Groups and 1AM Groups.
- C. Configure AWS as the relying party in Active Directory
- D. Configure AWS as the relying party in Active Directory Federation services

Answer: AD

Explanation:

The AWS Documentation mentions some key aspects with regards to the configuration of Onpremise AD with AWS

One is the Groups configuration in AD Active Directory Configuration

Determining how you will create and delineate your AD groups and 1AM roles in AWS is crucial to how you secure access to your account and manage resources. SAML assertions to the AWS environment and the respective 1AM role access will be managed through regular expression (regex) matching between your on-premises AD group name to an AWS 1AM role.

One approach for creating the AD groups that uniquely identify the AWS 1AM role mapping is by selecting a common group naming convention. For example, your AD groups would start with an identifier, for example, AWS-, as this will distinguish your AWS groups from others within the organization. Next include the 12-digit AWS account number. Finally, add the matching role name within the AWS account. Here is an example:

And next is the configuration of the relying party which is AWS

ADFS federation occurs with the participation of two parties; the identity or claims provider (in this case the owner of the identity repository - Active Directory) and the relying party, which is another application that wishes to outsource authentication to the identity provider; in this case Amazon Secure Token Service (STS).

The relying party is a federation partner that is represented by a claims provider trust in the federation service.

Option B is invalid because AD groups should not be matched to 1AM Groups

Option C is invalid because the relying party should be configured in Active Directory Federation services

For more information on the federated access, please visit the following URL:

1 <https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directoryfederation-services-ad-fs/>

The correct answers are: Ensure the right match is in place for On-premise AD Groups and 1AM Roles., Configure AWS as the relying party in Active Directory Federation services

Submit your Feedback/Queries to our Experts

NEW QUESTION 25

Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service? Please select:

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

Answer: B

Explanation:

On the AWS Blog site the following information is present to help on this context

The newly released whitepaper, Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can access AWS by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access AWS resources.

Option A, C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign-on.

For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL:

<https://aws.amazon.com/blogs/security/new-whitepaper-single-sign-on-integrating-aws-openldap-and-shibboleth/>

The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP. Submit your Feedback/Queries to our Experts

NEW QUESTION 30

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 CloudWatch 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 CloudWatch metrics to find for the suspicious activity which occurred 11 days ago
- D. Use AWS Config to get the API calls which were made 11 days ago

Answer: B

Explanation:

The CloudTrail 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 are invalid because CloudWatch is used for logging and not for monitoring API activity. Option D is invalid because AWS Config 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/userguide/how-cloudtrail-works.html>

Note:

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

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

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

NEW QUESTION 34

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 URLs
- 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 account 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 use 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-content-trusted-signers.html>

The correct answer is: Create pre-signed URLs. Submit your Feedback/Queries to our Experts

NEW QUESTION 37

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 38

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:V1aService to allow a user to use a customer managed CMK only for requests that Amazon S3 makes on their behalf. Or you can use it to deny the user permission to a CMK when a request on their behalf comes from AWS Lambda.

For more information on key policy's for KMS please visit the following URL: <https://docs.aws.amazon.com/kms/latest/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 40

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

Please select:

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

Answer: BC

Explanation:

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

Option A is invalid because databases should not be placed in the public subnet

Option D is invalid because the database security group should not allow traffic from the internet For more information on this type of setup, please refer to the below URL: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/PC_Scenario2.

The correct answers are: Place the EC2 Instance with the Oracle database in a separate private subnet Create a database security group and ensure the web security group to allowed incoming access

Submit your Feedback/Queries to our Experts

NEW QUESTION 41

An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users. Which of the following is a secure way of ensuring that the EC2 Instance access the Dynamo table

Please select:

- A. Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance
- B. Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- C. Use 1AM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- D. Use 1AM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance

Answer: A

Explanation:

To always ensure secure access to AWS resources from EC2 Instances, always ensure to assign a Role to the EC2 Instance Option B is invalid because KMS keys are not used as a mechanism for providing EC2 Instances access to AWS services. Option C is invalid Access keys is not a safe mechanism for providing EC2 Instances access to AWS services. Option D is invalid because there is no way access groups can be assigned to EC2 Instances. For more information on 1AM Roles, please refer to the below URL:

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

The correct answer is: Use 1AM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance Submit your Feedback/Queries to our Experts

NEW QUESTION 43

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

Please select:

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

G. Use AWS Config to enable the trail for all future region

Answer: B

Explanation:

The AWS Documentation mentions the following

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

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

Option D is invalid because this AWS Config cannot be used to enable trails For more information on this feature, please visit the following URL:

<https://aws.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-regions-and-support-for-multiple-trails>

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

NEW QUESTION 46

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 run. 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/monitoring-functions.html>

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

NEW QUESTION 48

A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest. How can this be achieved?

Please select:

- A. Use AWS Access keys to encrypt the data
- B. Use SSL certificates to encrypt the data
- C. Enable server side encryption on the S3 bucket
- D. Enable MFA on the S3 bucket

Answer: C

Explanation:

The AWS Documentation mentions the following

Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.

Options A and B are invalid because neither Access Keys nor SSL certificates can be used to encrypt data.

Option D is invalid because MFA is just used as an extra level of security for S3 buckets For more information on S3 server side encryption, please refer to the below Link: <https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

Submit your Feedback/Queries to our Experts

NEW QUESTION 52

Your company hosts critical data in an S3 bucket. There is a requirement to ensure that all data is encrypted. There is also metadata about the information stored in the bucket that needs to be encrypted as well. Which of the below measures would you take to ensure that the metadata is encrypted?

Please select:

- A. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server side encryption.
- B. Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server KMS encryption.
- C. Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time.
- D. Put the metadata in the S3 bucket itself

Answer: C

Explanation:

Option A ,B and D are all invalid because the metadata will not be encrypted in any case and this is a key requirement from the question.

One key thing to note is that when the S3 bucket objects are encrypted, the meta data is not encrypted. So the best option is to use an encrypted DynamoDB table Important

All GET and PUT requests for an object protected by AWS KMS will fail if they are not made via SSL or by using SigV4. SSE-KMS encrypts only the object data

A. Any object metadata is not encrypted. For

more information on using KMS encryption for S3, please refer to below URL: 1 <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

The correct answer is: Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time. Submit your Feedback/Queries to our Experts

NEW QUESTION 55

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%20Cybersecurity%20Framework.pdf)

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 58

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

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

Answer: D

Explanation:

Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances, the SSL termination should occur on the Ec2 Instances. Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application.

Option B is incorrect since encryption is required until the EC2 Instance

For more information on HTTPS listeners for classic load balancers, please refer to below URL

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-https-load-balancers.html> The correct answer is: Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances

Submit your Feedback/Queries to our Experts

NEW QUESTION 63

Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below
Please select:

- A. Use a host based intrusion detection system
- B. Use a third party firewall installed on a central EC2 instance
- C. Use VPC Flow logs
- D. Use Network Access control lists logging

Answer: AB

Explanation:

If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the AWS Security best practices

Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on AWS Security best practices, please refer to below URL:
The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2

Submit your Feedback/Queries to our Experts

NEW QUESTION 67

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

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

Answer: BD

Explanation:

The AWS Documentation mentions the following

All AWS accounts have root user credentials (that is, the credentials of the account owner). These credentials allow full access to all resources in the account.

Because you can't restrict permissions for root user credentials, we recommend that you delete your root user access keys. Then create AWS Identity and Access Management (IAM) user credentials for everyday interaction with AWS. Option A is incorrect since you cannot delete the root access account

Option C is partially correct but cannot be used as the ideal solution for safeguarding the account For more information on root access vs admin IAM users, please refer to below URL: <https://docs.aws.amazon.com/eeneral/latest/er/root-vs-iam.html>

The correct answers are: Create an Admin IAM user with the necessary permissions. Delete the root access keys Submit your Feedback/Queries to our Experts

NEW QUESTION 72

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

Please select:

- A. AWS Cognito
- B. AWS SAML
- C. AWS IAM
- D. AWS Config

Answer: A

Explanation:

The AWS Documentation mentions the following

Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, or Google.

Option B is incorrect since this is used for identity federation

Option C is incorrect since this is pure Identity and Access management Option D is incorrect since AWS is a configuration service

For more information on AWS Cognito please refer to the below Link: <https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html>

The correct answer is: AWS Cognito

Submit your Feedback/Queries to our Experts

NEW QUESTION 73

Your application currently uses 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 would 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/cognito/latest/developerguide/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 74

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

Please select:

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

Answer: BC

Explanation:

The AWS Documentation mentions the following

You can configure multiple trails differently so that the trails process and log only the events that you specify. For example, one trail can log read-only data and management events, so that all read-only events are delivered to one S3 bucket. Another trail can log only write-only data and management events, so that all write-only events are delivered to a separate S3 bucket

Options A and D are invalid because you have to create a trail and not a log group

For more information on managing events with CloudTrail, please visit the following URL:

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/loHEing-manasement-and-dataevents- with-cloudtrai>

The correct answers are: Create one trail that logs data events to an S3 bucket. Create another trail that logs management events to another S3 bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 78

Your company has been using AWS for hosting EC2 Instances for their web and database applications. They want to have a compliance check to see the

following

Whether any ports are left open other than admin ones like SSH and RDP

Whether any ports to the database server other than ones from the web server security group are

open Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?

Please select:

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

Answer: B

Explanation:

Trusted Advisor checks for compliance with the following security recommendations:

Limited access to common administrative ports to only a small subset of addresses. This includes ports 22 (SSH), 23 (Telnet) 3389 (RDP), and 5500 (VNC).

Limited access to common database ports. This includes ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) and 5432 (PostgreSQL).

Option A is partially correct but then you would need to write custom rules for this. The AWS trusted advisor can give you all o these checks on its dashboard

Option C is incorrect. Amazon Inspector needs a software agent to be installed on all EC2 instances that are included in th.

assessment target, the security of which you want to evaluate with Amazon Inspector. It monitors the behavior of the EC2

instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and

configuration data (telemetry), which it then passes to the Amazon Inspector service.

Our question's requirement is to choose a choice that is easy to implement. Hence Trusted Advisor is more appropriate for this) question.

Options D is invalid because this service dont provide these details.

For more information on the Trusted Advisor, please visit the following URL <https://aws.amazon.com/premiumsupport/trustedadvisor>>

The correct answer is: AWS Trusted Advisor Submit your Feedback/Queries to our Experts

NEW QUESTION 81

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at

Rest. If the user is supplying his own keys for encryption SSE-C, which of the below mentioned statements is true?

Please select:

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

Answer: B

Explanation:

.anaging your own encryption keys, y

You can encrypt the object and send it across to S3

Option A is invalid because ideally you should use different encryption keys Option C is invalid because you can use you own encryption keys Option D is invalid

because encryption works even if versioning is enabled For more information on client side encryption please visit the below Link: ""Keys.html

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

The correct answer is: It is possible to have different encryption keys for different versions of the same object Submit your Feedback/Queries to our Experts

NEW QUESTION 85

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 87

In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being recreated.

What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below

Please select:

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

Answer: D

Explanation:

One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective. The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3. Options A,B and C are all invalid because you should not give access to the developers on the Apache server. For more information on S3, please refer to the below link <https://aws.amazon.com/documentation/s3>. The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access. Submit your Feedback/Queries to our Experts

NEW QUESTION 90

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

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

Answer: C

Explanation:

The AWS Documentation mentions the following
A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.
User pools provide:
Sign-up and sign-in services.
A built-in, customizable web UI to sign in users.
Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.
User directory management and user profiles.
Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
Customized workflows and user migration through AWS Lambda triggers. Options A and B are invalid because these are not used to manage users. Option D is invalid because this would be a maintenance overhead.
For more information on Cognito User Identity pools, please refer to the below Link: <https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html>
The correct answer is: Use AWS Cognito to manage the user profiles. Submit your Feedback/Queries to our Experts

NEW QUESTION 91

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

- 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-aws-organization-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 96

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 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 to 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 100

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

Please select:

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

Answer: AB

Explanation:

Option C is invalid because the instances need to remain in the private: Option D is invalid because AWS inspector can only detect the patches

One of the AWS Blogs mentions how patching of Linux servers can be accomplished. Below is the diagram representation of the architecture setup

For more information on patching Linux workloads in AWS, please refer to the Lin. <https://aws.amazon.com/blogs/security/how-to-patch-linux-workloads-on-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 105

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

Please select:

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

Answer: D

Explanation:

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

Option A is invalid because you need to use Cloudwatch Events to check for chan, Option B is invalid because you need to use Cloudwatch Events to check for chang

Option C is invalid because AWS inspector is not used to monitor the activity on Security Groups For more information on monitoring security groups, please visit the below URL: <https://aws.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notificationsabout-changes-to-your-amazonjpc-security-groups/>

The correct answer is: Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well. Submit your Feedback/Queries to our Experts

NEW QUESTION 109

There is a requirement for a company to transfer large amounts of data between AWS and an onpremise location. There is an additional requirement for low latency and high consistency traffic to

AWS. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

Please select:

- A. Provision a Direct Connect connection to an AWS region using a Direct Connect partner.
- B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.
- C. Create an IPSec tunnel for private connectivity, which increases network consistency and reduces latency.

D. Create a VPC peering connection between AWS and the Customer gatewa

Answer: A

Explanation:

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect you can establish private connectivity between AWS and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than InternetQuestions

& Answers PDF P-140 based connections.

Options B and C are invalid because these options will not reduce network latency Options D is invalid because this is only used to connect 2 VPC's

For more information on AWS direct connect, just browse to the below URL: <https://aws.amazon.com/directconnect>

The correct answer is: Provision a Direct Connect connection to an AWS region using a Direct Connect partner. omit your Feedback/Queries to our Experts

NEW QUESTION 112

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

Please select:

A. Add an AWS managed policy for the user

B. Add a service policy for the user

C. Add an 1AM role for the user

D. Add an inline policy for the user

Answer: D

Explanation:

Options A and B are incorrect since you need to add an inline policy just for the user Option C is invalid because you don't assign an 1AM role to a user

The AWS Documentation mentions the following

An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.

For more information on 1AM Access and Inline policies, just browse to the below URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/access>

The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

NEW QUESTION 115

Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?

Please select:

A. Use CloudTrail Log File Integrity Validation.

B. Use AWS Config SNS Subscriptions and process events in real time.

C. Use CloudTrail backed up to AWS S3 and Glacier.

D. Use AWS Config Timeline forensic

Answer: A

Explanation:

The AWS Documentation mentions the following

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

Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs

For more information on Cloudtrail log file validation, please visit the below URL: <http://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> The correct answer is: Use CloudTrail Log File Integrity Validation.

omit your Feedback/Queries to our Expert

NEW QUESTION 120

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

Please select:

A. Use S3 SSE and use SSL for data in transit

B. SSL termination on the ELB

C. Enabling Proxy Protocol

D. Enabling sticky sessions on your load balancer

Answer: A

Explanation:

By disabling SSL termination, you are leaving an unsecure connection from the ELB to the back end instances. Hence this means that part of the data transit is not being encrypted.

Option B is incorrect because this would not guarantee complete encryption of data in transit Option C and D are incorrect because these would not guarantee encryption

For more information on SSL Listeners for your load balancer, please visit the below URL: <http://docs.aws.amazon.com/elasticloadbalancine/latest/classic/elb-https-load-balancers.html> The correct answer is: Use S3 SSE and use SSL for data in transit

Submit your Feedback/Queries to our Experts

NEW QUESTION 121

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-Security-Specialty Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-Certified-Security-Specialty Product From:

<https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/>

Money Back Guarantee

AWS-Certified-Security-Specialty Practice Exam Features:

- * AWS-Certified-Security-Specialty Questions and Answers Updated Frequently
- * AWS-Certified-Security-Specialty Practice Questions Verified by Expert Senior Certified Staff
- * AWS-Certified-Security-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * AWS-Certified-Security-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year