

Exam Jan 4 set B

Total points 56/65 ?

Full Marks : 65

Pass Marks : 47

Time :120 minutes

Email *

07yamini2055@gmail.com

0 of 0 points

Full Name *

Ira Chand

All Questions are Compulsary

56 of 65 points

✓ Which AWS security service provides a firewall at the subnet level within a VPC? *1/1

- ☐ Bucket Policy
- ☐ Security Group
- ☒ Network Access Control List
- ☐ IAM Policy



Feedback

Explanation

A Network ACL is a firewall that is associated with a subnet within your VPC. It is used to filter the network traffic that enters and exits the subnet.

CORRECT: "Network Access Control List" is the correct answer.

INCORRECT: "Security Group" is incorrect. A Security Group is a firewall that is associated with an EC2 instances (not the subnet). Security Groups control the traffic the inbound and outbound network traffic from/to the instance.

INCORRECT: "IAM Policy" is incorrect. An IAM Policy is used to assign permissions to users and roles.

INCORRECT: "Bucket Policy" is incorrect. A Bucket Policy is used with Amazon S3 buckets to control access.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

✗ Which feature of AWS IAM enables you to identify unnecessary permissions that have been assigned to users?

*0/1

- ☐ Access Advisor
- ☐ Role Advisor
- ☒ Permissions Advisor
- ☐ Group Advisor

✗

Correct answer

- ☒ Access Advisor

Feedback

Explanation

The IAM console provides information about when IAM users and roles last attempted to access AWS services. This information is called service last accessed data. This data can help you identify unnecessary permissions so that you can refine your IAM policies to better adhere to the principle of "least privilege."

That means granting the minimum permissions required to perform a specific task. You can find the data on the Access Advisor tab in the IAM console by examining the detail view for any IAM user, group, role, or managed policy.

CORRECT: "Access Advisor" is the correct answer.

INCORRECT: "Role Advisor" is incorrect as this is not a valid feature.

INCORRECT: "Permissions Advisor" is incorrect as this is not a valid feature.

INCORRECT: "Group Advisor" is incorrect as this is not a valid feature.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_access-

✗ Your manager has asked you to explain the benefits of using IAM groups. *0/1
Which of the below statements are valid benefits? (Select TWO.)

- ☒ Provide the ability to create custom permission policies ✗
- ☐ Provide the ability to nest groups to create an organizational hierarchy
- ☐ Enables you to attach IAM permission policies to more than one user at a time
- ☐ You can restrict access to the subnets in your VPC
- ☒ Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users ✓

Correct answer

- ☒ Enables you to attach IAM permission policies to more than one user at a time
- ☒ Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users

Feedback

Explanation

Groups are collections of users and have policies attached to them. This enables you to organize groups of users by job function or role and apply relevant policies to the group.

You can use groups to assign permissions to users and should follow the principal of least privilege when assigning permissions.

CORRECT: "Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users" is a correct answer.

CORRECT: "Enables you to attach IAM permission policies to more than one user at a time" is also a correct answer.

INCORRECT: "You can restrict access to the subnets in your VPC" is incorrect as this describes Network ACLs.

INCORRECT: "Provide the ability to create custom permission policies" is incorrect as this describes IAM policies.

INCORRECT: "Provide the ability to nest groups to create an organizational hierarchy" is incorrect. You cannot nest groups (groups within groups).

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html>

✓ A company wants to utilize a pay as you go cloud model for all of their applications without CAPEX costs and which is highly elastic. Which cloud delivery model will suit them best? *1/1

- ☐ Hybrid
- ☐ Private
- ☐ On-premise
- ☒ Public



Feedback

Explanation

The public cloud is offered under a purely pay as you go model (unless you choose to reserve), and allows companies to completely avoid CAPEX costs. The public cloud is also highly elastic so companies can grow and shrink the applications as demand changes.

Private and on-premise clouds are essentially the same, though both could be managed by a third party and even could be delivered under an OPEX model by some vendors. However, they are typically more CAPEX heavy and the elasticity is limited.

A hybrid model combines public and private and this company wants to go all in on a single model.

CORRECT: "Public" is the correct answer.

INCORRECT: "Private" is incorrect as explained above.

INCORRECT: "Hybrid" is incorrect as explained above.

INCORRECT: "On-premise" is incorrect as explained above.

References:

<https://aws.amazon.com/types-of-cloud-computing/>

✓ Which of the statements below does NOT characterize cloud computing? * 1/1

- ☒ Cloud computing allows you to swap variable expense for capital expense ✓
- ☐ With cloud computing you can increase your speed and agility
- ☐ Cloud computing is the on-demand delivery of compute power
- ☐ With cloud computing you get to benefit from massive economies of scale

Feedback

Explanation

Cloud computing is not a one-off capital expense, it is an ongoing operating expense. The caveat to this is that if you purchase reserved capacity you have an option to partially or fully pay upfront. However, it is still an operating cost as you do not own and depreciate the assets.

CORRECT: "Cloud computing allows you to swap variable expense for capital expense" is the correct answer.

INCORRECT: "Cloud computing is the on-demand delivery of compute power" is incorrect as this is a valid statement.

INCORRECT: "With cloud computing you get to benefit from massive economies of scale" is incorrect as this is a valid statement.

INCORRECT: "With cloud computing you can increase your speed and agility" is incorrect as this is a valid statement.

References:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html>

✓ Your manager has asked you to explain some of the security features available in the AWS cloud. How can you describe the function of Amazon CloudHSM? *1/1

- ☒ It can be used to generate, use and manage encryption keys in the cloud ✓
- ☐ It is a Public Key Infrastructure (PKI)
- ☐ It provides server-side encryption for S3 objects
- ☐ It is a firewall for use with web applications

Feedback

Explanation

AWS CloudHSM is a cloud-based hardware security module (HSM) that allows you to easily add secure key storage and high-performance crypto operations to your AWS applications.

CloudHSM has no upfront costs and provides the ability to start and stop HSMs on-demand, allowing you to provision capacity when and where it is needed quickly and cost-effectively.

CloudHSM is a managed service that automates time-consuming administrative tasks, such as hardware provisioning, software patching, high availability, and backups.

CORRECT: "It can be used to generate, use and manage encryption keys in the cloud" is the correct answer.

INCORRECT: "It provides server-side encryption for S3 objects" is incorrect. CloudHSM performs key management but it does not perform encryption of S3 objects.

INCORRECT: "It is a Public Key Infrastructure (PKI)" is incorrect. It can be used to generate asymmetric keys, however it is not a PKI.

INCORRECT: "It is a firewall for use with web applications" is incorrect as it does not provide any firewall functionality.

References:

<https://aws.amazon.com/cloudhsm/details/>

✓ Which AWS security tool uses an agent installed in EC2 instances and assesses applications for vulnerabilities and deviations from best practices? *1/1

- ☒ AWS Inspector ✓
- ☐ AWS Trusted Advisor
- ☐ AWS Personal Health Dashboard
- ☐ AWS TCO Calculator

Feedback

Explanation

Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Inspector automatically assesses applications for vulnerabilities or deviations from best practices. Inspector uses an agent installed on EC2 instances.

CORRECT: "AWS Inspector" is the correct answer.

INCORRECT: "AWS Trusted Advisor" is incorrect. Trusted Advisor is an online resource that helps to reduce cost, increase performance and improve security by optimizing your AWS environment.

INCORRECT: "AWS Personal Health Dashboard" is incorrect. AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you.

INCORRECT: "AWS TCO Calculator" is incorrect. The AWS TCO calculator can be used to compare the cost of running your applications in an on-premises or colocation environment to AWS.

References:

<https://aws.amazon.com/inspector/>

✓ Which service allows you to monitor and troubleshoot systems using system and application log files generated by those systems? *1/1

- ☒ CloudWatch Logs
- ☐ CloudTrail Logs
- ☐ CloudTrail Metrics
- ☐ CloudWatch Metrics



Feedback

Explanation

Amazon CloudWatch Logs lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files. CloudWatch Logs can be used for real time application and system monitoring as well as long term log retention.

CORRECT: "CloudWatch Logs" is the correct answer.

INCORRECT: "CloudTrail Logs" is incorrect. CloudTrail is used for logging who does what in AWS by recording API calls. It is used for auditing, not performance or system operational monitoring.

INCORRECT: "CloudWatch Metrics" is incorrect. CloudWatch metrics are the standard method by which CloudWatch collects data

INCORRECT: "CloudTrail Metrics" is incorrect. CloudTrail does not record metrics, it records logs.

References:

<https://aws.amazon.com/cloudtrail/>

✗ Which HTTP code indicates a successful upload of an object to Amazon S3? *0/1

☒ 400

✗

☐ 500

☐ 300

☐ 200

Correct answer

☒ 200

Feedback

Explanation

HTTP response status codes indicate whether a specific HTTP request has been successfully completed.

- A HTTP 200 codes indicates a successful upload.

- A HTTP 300 code indicates a redirection.

- A HTTP 400 code indicates a client error.

- A HTTP 500 code indicates a server error.

CORRECT: "200" is the correct answer.

INCORRECT: "300" is incorrect as explained above.

INCORRECT: "400" is incorrect as explained above.

INCORRECT: "500" is incorrect as explained above.

References:

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

✓ Which AWS feature of Amazon EC2 allows an administrator to create a standardized image that can be used for launching new instances? *1/1

- ☒ Amazon Machine Image
- ☐ Amazon Block Template
- ☐ Amazon Golden Image
- ☐ Amazon EBS Mount Point



Feedback

Explanation

An Amazon Machine Image (AMI) provides the information required to launch an instance. You can use an AMI to launch identical instances from a standard template. This is also known as a Golden Image (though no such feature exists in AWS with this name). An AMI is created from an EBS snapshot and also includes launch permissions and a block device mapping.

CORRECT: "Amazon Machine Image" is the correct answer.

INCORRECT: "Amazon Golden Image" is incorrect as this is not an AWS feature.

INCORRECT: "Amazon Block Template" is incorrect. Amazon Block Templates do not exist.

INCORRECT: "Amazon EBS Mount Point" is incorrect. An Amazon EBS Mount Point is not an AWS feature. You do mount EBS volumes however this is within the operating system. Block device mappings are used in AMIs to specify how to mount the EBS volume.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>

✓ What advantages does the AWS cloud provide in relation to cost? (Select *1/1 TWO.)

- ☐ Itemized power costs
- ☒ Ability to turn off resources and not pay for them
- ☒ Fine-grained billing
- ☐ One-off payments for on-demand resources
- ☐ Enterprise licensing discounts



Feedback

Explanation

With the AWS cloud you get fine-grained billing and can turn off resources you are not using easily and not have to pay for them (pay for what you use model).

CORRECT: "Fine-grained billing" is a correct answer.

CORRECT: "Ability to turn off resources and not pay for them" is also a correct answer.

INCORRECT: "One-off payments for on-demand resources" is incorrect. You do not get the option for one-off payments for on-demand resources. You can for reserved instances which can be paid all upfront.

INCORRECT: "Enterprise licensing discounts" is incorrect. You do not get enterprise licensing discounts from AWS and you do not pay anything for power as the cost is built in.

INCORRECT: "Itemized power costs" is incorrect. You do not get any power costs on your bill

References:

<https://aws.amazon.com/ec2/pricing/>

✓ How can a systems administrator specify a script to be run on an EC2 instance during launch? *1/1

- ☐ AWS Config
- ☒ User Data
- ☐ Run Command
- ☐ Metadata



Feedback

Explanation

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts.

You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives. User data is data that is supplied by the user at instance launch in the form of a script. User data is limited to 16KB. User data and meta data are not encrypted.

CORRECT: "User Data" is the correct answer.

INCORRECT: "Metadata" is incorrect as metadata retrieves information about the instance.

INCORRECT: "Run Command" is incorrect as this operates separately to the launch process.

INCORRECT: "AWS Config" is incorrect as this service stores configuration information relating to AWS services.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html>

✓ Which pricing model will interrupt a running Amazon EC2 instance if capacity becomes temporarily unavailable? *1/1

- ☐ Standard Reserved Instances
- ☐ Convertible Reserved Instances
- ☒ Spot Instances
- ☐ On-Demand Instances



Feedback

Explanation

Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices. When AWS need to reclaim the capacity you get a 2 minute warning and then your instances are terminated.

With all other pricing models your instances will not be terminated by AWS once they are running.

CORRECT: "Spot Instances" is the correct answer.

INCORRECT: "On-Demand Instances" is incorrect as explained above.

INCORRECT: "Standard Reserved Instances" is incorrect as explained above.

INCORRECT: "Convertible Reserved Instances" is incorrect as explained above.

References:

<https://aws.amazon.com/ec2/spot/>

✗ Which AWS service is suitable for an event-driven workload? *

0/1

- ☐ Amazon Open 3D Engine
- ☐ Amazon EC2
- ☐ AWS Lambda
- ☒ AWS Elastic Beanstalk

✗

Correct answer

- ☒ AWS Lambda

Feedback

Explanation

AWS Lambda is an event-driven service. For example you can configure an Amazon S3 bucket with event notifications that trigger an AWS Lambda function when data is uploaded to an S3 bucket.

CORRECT: "AWS Lambda" is the correct answer.

INCORRECT: "Amazon EC2" is incorrect as this is not an event-driven service.

INCORRECT: "AWS Elastic Beanstalk" is incorrect as this is not an event-driven service.

INCORRECT: "Amazon Open 3D Engine" is incorrect as this is a game engine service.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html>

✓ What does an organization need to do in Amazon IAM to enable user access to services being launched in new region? *1/1

- ☐ Update the user accounts to allow access from another region
- ☒ Nothing, IAM is global ✓
- ☐ Enable global mode in IAM to provision the required access
- ☐ Create new user accounts in the new region

Feedback

Explanation

IAM is used to securely control individual and group access to AWS resources. IAM is universal (global) and does not apply to regions.

CORRECT: "Nothing, IAM is global" is the correct answer.

INCORRECT: "Enable global mode in IAM to provision the required access" is incorrect as you do not need to do anything to use IAM globally.

INCORRECT: "Update the user accounts to allow access from another region" is incorrect as you don't need to update user accounts.

INCORRECT: "Create new user accounts in the new region" is incorrect as IAM is global.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

✗ A cloud practitioner needs to decrease application latency and increase performance for globally distributed users. *0/1

Which services can assist? (Select TWO.)

☐ Amazon ECS

☒ Amazon ElastiCache

✗

☒ Amazon CloudFront

✓

☐ Amazon S3

☐ Amazon AppStream 2.0

Correct answer

☒ Amazon CloudFront

☒ Amazon S3

Feedback

Explanation

Amazon S3 is an object-based storage system. It can be used to store data such as files and images that need to be served. Optionally, an S3 bucket can be configured as a static website. Amazon CloudFront is a content delivery network (CDN) that caches content at Edge Locations around the world.

These two services can work together with an S3 bucket configured as an origin for the CloudFront distribution. Users around the world will then be able to pull the content from the local Edge Location with lower latency and better performance.

CORRECT: "Amazon S3" is a correct answer.

CORRECT: "Amazon CloudFront" is also a correct answer.

INCORRECT: "Amazon ECS" is incorrect. The Elastic Container Service (ECS) is used for running Docker containers on AWS. This is not going to help with reducing latency or increasing performance for global users.

INCORRECT: "Amazon AppStream 2.0" is incorrect. This is an application streaming service for streaming applications to computers. It is unsuitable for these requirements.

INCORRECT: "Amazon ElastiCache" is incorrect. ElastiCache caches data from a database in-memory. It is unsuitable for these requirements.

References:

<https://aws.amazon.com/cloudfront/>

✓ Which of the following are advantages of using the AWS cloud computing *1/1 over legacy IT? (Select TWO.)

- ☒ You don't need to worry about over provisioning as you can elastically scale ✓
- ☒ You can bring new applications to market faster ✓
- ☐ You don't need to patch your operating systems
- ☐ You are able to pass responsibility for the availability of your application to AWS
- ☐ You can bring services closer to your end users

Feedback

Explanation

With cloud computing you no longer need to guess about capacity as you can elastically scale. This means you don't end up overprovisioning but instead react to the load on your servers. You can also be faster and more agile with development and release of applications.

CORRECT: "You don't need to worry about over provisioning as you can elastically scale" is a correct answer.

CORRECT: "You can bring new applications to market faster" is also a correct answer.

INCORRECT: "You are able to pass responsibility for the availability of your application to AWS" is incorrect. You do not pass responsibility for your application to AWS. AWS runs the infrastructure but you still manage the application

INCORRECT: "You don't need to patch your operating systems" is incorrect. You still need to patch your own operating systems.

INCORRECT: "You can bring services closer to your end users" is incorrect. The cloud is centralized so you won't necessarily bring services closer to your end users.

References:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html>

- ✓ A company needs significant cost savings for their non-interruptible workloads on AWS. *1/1

Which EC2 instance pricing model should the company select?

- ☐ On-Demand Instances
- ☒ Reserved Instances
- ☐ Dedicated Hosts
- ☐ Spot Instances



Feedback

Explanation

Reserved instances allow a customer to use on-demand EC2 instances at a discounted price based on a commitment of usage. If you require cost optimization of non-interruptible workloads, you can use Reserved instances to provide discounts on your EC2 spend.

CORRECT: "Reserved instances" is the correct answer (as explained above.)

INCORRECT: "On-Demand Instances" is incorrect as On-demand instances are the most expensive, and the default billing option for EC2 instances. The customer requires significant cost savings, which cannot be provided by on-demand instances.

INCORRECT: "Spot Instances" is incorrect. Spot Instances are not suitable as spot instances let you take advantage of unused EC2 capacity in the AWS cloud, which can be terminated at a 2-minute notice if AWS requires the capacity for on-demand customers.

INCORRECT: "Dedicated Hosts" is incorrect, as this is a specific billing option if you require a dedicated server for server-bound-licenses. This is not required for this use case and is an expensive EC2 pricing option.

References:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

- ✓ A system administrator discovers that several Amazon EC2 instances have been terminated. It is the responsibility of the system administrator to identify the user or AWS API call that terminated these instances. *1/1

Which AWS service should the system administrator use to meet this requirement?

- ☐ Amazon Inspector
- ☐ AWS Trusted Advisor
- ☒ AWS CloudTrail
- ☐ Amazon Detective



Feedback

Explanation

AWS CloudTrail tracks API calls that are made within a particular AWS account. It will track the API call made, the IP address it originated from and which IAM principal initiated the action.

CORRECT: "AWS CloudTrail" is the correct answer (as explained above.)

INCORRECT: "AWS Trusted Advisor" is incorrect. AWS Trusted Advisor provides recommendations that help you follow AWS best practices. Trusted Advisor evaluates your account by using checks. These checks identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas. You can then follow the check recommendations to optimize your services and resources.

INCORRECT: "Amazon Inspector" is incorrect. Inspector is a fully managed vulnerability assessment tool, which doesn't track who is performing what actions within an account.

INCORRECT: "Amazon Detective" is incorrect. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations. It does not however track API calls within an account.

References:

<https://aws.amazon.com/cloudtrail/>

✓ According to the AWS Shared Responsibility Model, which of the following is a shared control?

*1/1

- ☐ Operating system patching
- ☐ Protection of infrastructure
- ☒ Awareness and training
- ☐ Client-side data encryption



Feedback

Explanation

Shared Controls are controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include patch management, configuration management, and awareness and training.

CORRECT: "Awareness and training" is the correct answer.

INCORRECT: "Operating system patching" is incorrect. Though patch management is a shared control, operating system patching specifically is a customer responsibility.

INCORRECT: "Protection of infrastructure" is incorrect. Protection of infrastructure is solely an AWS responsibility.

INCORRECT: "Client-side data encryption" is incorrect. Client and server-side data encryption are both customer responsibilities.

References:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

✓ How can you deploy your EC2 instances so that if a single data center fails you still have instances available? *1/1

- ☐ Across regions
- ☐ Across VPCs
- ☐ Across subnets
- ☒ Across Availability Zones



Feedback

Explanation

An AZ spans one or more data centers and each AZ is physically isolated from other AZs and connected by high speed networking. If you want to deploy a highly available application you should spread your instances across AZs and they will be resilient to the failure of a single DC

CORRECT: "Across Availability Zones" is the correct answer.

INCORRECT: "Across regions" is incorrect. You could deploy your instances across separate regions but this is not necessary to create a highly available application and introduces complexity and cost. For example you may need multiple ELBs (one per region), complex name resolution and potential data transfer charges.

INCORRECT: "Across subnets" is incorrect. Subnets are created within AZs. Therefore, if you deploy resources into multiple subnets within an AZ and a data center fails, you may lose all of your instances.

INCORRECT: "Across VPCs" is incorrect. You should deploy across AZs within a VPC.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

✗ Which of the following are included in AWS Enterprise Support? (Choose two.) *0/1

- ☒ AWS technical account manager (TAM) ✓
- ☐ AWS partner-led support
- ☐ AWS Professional Services
- ☐ Support of third-party software integration to AWS
- ☒ 5-minute response time for critical issues ✗

Correct answer

- ☒ AWS technical account manager (TAM)
- ☒ Support of third-party software integration to AWS

Feedback

Designated point of contact

A Technical Account Manager (TAM) is your designated technical point of contact who helps you onboard, provides advocacy and guidance to help plan and build solutions using best practices, coordinates access to subject matter experts, assists with case management, presents insights and recommendations on your AWS spend, workload optimization, and event management, and proactively keeps your AWS environment healthy.

Third-party software support

Guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

✓ Which of the following descriptions is incorrect in relation to the design of Availability Zones? *1/1

- ☐ AZs are physically separated within a typical metropolitan region and are located in lower risk flood plains
- ☐ Each AZ is designed as an independent failure zone
- ☒ Each subnet in a VPC is mapped to all AZs in the region ✓
- ☐ AZ's have direct, low-latency, high throughput and redundant network connections between each other

Feedback

Explanation

Subnets are created within a single AZ and do not get mapped to multiple AZs.

CORRECT: "Each subnet in a VPC is mapped to all AZs in the region" is the correct answer.

INCORRECT: "AZ's have direct, low-latency, high throughput and redundant network connections between each other" is incorrect as this is true.

INCORRECT: "Each AZ is designed as an independent failure zone" is incorrect as this is true.

INCORRECT: "AZs are physically separated within a typical metropolitan region and are located in lower risk flood plains" is incorrect as this is true.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

✓ Under the AWS shared responsibility model, which of the following are customer responsibilities? (Select TWO.) *1/1

- ☒ Setting up server-side encryption on an Amazon S3 bucket ✓
- ☒ Network and firewall configurations ✓
- ☐ Amazon RDS instance patching
- ☐ Physical security of data center facilities
- ☐ Compute capacity availability

Feedback

Explanation

As a customer on AWS you take responsibility for encrypting data. This includes encrypting data at rest and data in transit. Another security responsibility the customer owns is setting network and firewall configurations. For instance, you must configure Network ACLs and Security Groups and any operating system-level firewalls on your EC2 instances.

CORRECT: "Setting up server-side encryption on an Amazon S3 bucket" is a correct answer.

CORRECT: "Network and firewall configurations" is also a correct answer.

INCORRECT: "Amazon RDS instance patching" is incorrect. With RDS you can define the maintenance window but AWS actually perform the patching for you.

INCORRECT: "Physical security of data center facilities" is incorrect as this is security of the cloud and is an AWS responsibility.

INCORRECT: "Compute capacity availability" is incorrect as this is an AWS responsibility.

References:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

✓ What is an Edge location? *

1/1

- ☐ A public endpoint for Amazon S3
- ☒ A content delivery network (CDN) endpoint for CloudFront
- ☐ A VPC peering connection endpoint
- ☐ A virtual private gateway for VPN



Feedback

Explanation

Edge locations are Content Delivery Network (CDN) endpoints for CloudFront. There are many more edge locations than regions.

CORRECT: "A content delivery network (CDN) endpoint for CloudFront" is the correct answer.

INCORRECT: "A public endpoint for Amazon S3" is incorrect as it is not related to S3.

INCORRECT: "A virtual private gateway for VPN" is incorrect as it is not related to VPN.

INCORRECT: "A VPC peering connection endpoint" is incorrect as it is not related to VPC.

✓ Which AWS support plan provides email only support by Cloud Support Associates? *1/1

- ☐ Basic
- ☒ Developer
- ☐ Business
- ☐ Enterprise



Feedback

Explanation

Developer provides email support by the Cloud Support Associates team whereas Business and Enterprise provide email, 24x7 phone and chat access to Cloud Support Engineers. Basic does not provide email support at all.

CORRECT: "Developer" is the correct answer.

INCORRECT: "Basic" is incorrect as explained above.

INCORRECT: "Business" is incorrect as explained above.

INCORRECT: "Enterprise" is incorrect as explained above.

References:

<https://aws.amazon.com/premiumsupport/plans/>

✓ Which feature of Amazon S3 enables you to create rules to control the transfer of objects between different storage classes? *1/1

- ☐ Bucket policies
- ☐ Object sharing
- ☐ Versioning
- ☒ Lifecycle management



Feedback

Explanation

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

- *Transition actions*—Define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.
- *Expiration actions*—Define when objects expire. Amazon S3 deletes expired objects on your behalf. The lifecycle expiration costs depend on when you choose to expire objects.

CORRECT: "Lifecycle management" is the correct answer.

INCORRECT: "Object sharing" is incorrect. Object sharing refers to the ability to make any object publicly available via a URL.

INCORRECT: "Versioning" is incorrect. Versioning enabled you to automatically keep multiple versions of an object (when enabled).

INCORRECT: "Bucket policies" is incorrect. Bucket policies are used for controlling access to buckets, they can't be used to move data between storage classes.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

✓ Which type of EBS volumes can be encrypted? *

1/1

- ☒ Both non-root and root volumes ✓
- ☐ Only non-root volumes created from snapshots
- ☐ Only root volumes can have encryption applied at launch time
- ☐ Non-root volumes only

Feedback

Explanation

Amazon EBS encryption offers a straight-forward encryption solution for your EBS resources that doesn't require you to build, maintain, and secure your own key management infrastructure. It uses AWS Key Management Service (AWS KMS) customer master keys (CMK) when creating encrypted volumes and snapshots.

Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

All volumes can now be encrypted at launch time and it's possible to set this as the default setting.

CORRECT: "Both non-root and root volumes" is the correct answer.

INCORRECT: "Non-root volumes only" is incorrect as this is not true.

INCORRECT: "Only non-root volumes created from snapshots" is incorrect as you can encrypt all EBS volumes whether created from snapshots or not.

INCORRECT: "Only root volumes can have encryption applied at launch time" is incorrect as all volumes can have encryption applied at launch time.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

✓ What is the easiest way to store a backup of an EBS volume on Amazon S3? *1/1

- ☐ Use S3 lifecycle actions to backup the volume
- ☐ Write a custom script to copy the data into a bucket
- ☐ Use Amazon Kinesis to process the data and store the results in S3
- ☒ Create a snapshot of the volume



Feedback

Explanation

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.

CORRECT: "Create a snapshot of the volume" is the correct answer.

INCORRECT: "Write a custom script to copy the data into a bucket" is incorrect. Writing a custom script could work but would not be the easiest method.

INCORRECT: "Use S3 lifecycle actions to backup the volume" is incorrect. You cannot apply S3 lifecycle actions to EBS volumes.

INCORRECT: "Use Amazon Kinesis to process the data and store the results in S3" is incorrect. Amazon Kinesis is used for processing streaming data, not data in EBS volumes.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

- ✓ startup eCommerce company needs to quickly deliver new website features in an iterative manner, minimizing the time to market. *1/1

Which AWS Cloud feature allows this?

- ☐ Reliability
- ☐ High availability
- ☒ Agility ✓
- ☐ Elasticity

Feedback

Explanation

In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes.

This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

CORRECT: "Agility" is the correct answer.

INCORRECT: "High availability" is incorrect as this is associated with increased resilience, not agility.

INCORRECT: "Elasticity" is incorrect as this associated with the ability to adjust to demand and reduce the need to guess capacity requirements.

INCORRECT: "Reliability" is incorrect as this does not assist with bringing features to market faster.

References:

<https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html>

✓ Which AWS service is part of the suite of "serverless" services and runs code as functions? *1/1

☐ Amazon EKS

☐ AWS CodeCommit

☐ Amazon ECS

☒ AWS Lambda



Feedback

Explanation

AWS Lambda is a serverless compute service that runs your code in response to events and automatically manages the underlying compute resources for you. The code you run on AWS Lambda is called a "Lambda function".

CORRECT: "AWS Lambda" is the correct answer.

INCORRECT: "Amazon ECS" is incorrect. Amazon ECS is used for running software containers such as Docker containers.

INCORRECT: "Amazon EKS" is incorrect. Amazon EKS is used for managing software containers such as Docker containers.

INCORRECT: "AWS CodeCommit" is incorrect. AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories.

References:

<https://aws.amazon.com/lambda/>

<https://aws.amazon.com/lambda/features/>

✓ Under the shared responsibility model, which of the following tasks are the responsibility of the AWS customer? (Select TWO.) *1/1

- ☒ Ensuring that application data is encrypted at rest ✓
- ☐ Ensuring that AWS NTP servers are set to the correct time
- ☐ Ensuring that hardware is disposed of properly
- ☒ Ensuring that users have received security training in the use of AWS services ✓
- ☐ Ensuring that access to data centers is restricted

Feedback

Explanation

As a customer on AWS you take responsibility for encrypting data. This includes encrypting data at rest and data in transit. It's also a customer's responsibility to properly train their staff in security best practices and procedures for the AWS services they use.

CORRECT: "Ensuring that application data is encrypted at rest" is a correct answer.

CORRECT: "Ensuring that users have received security training in the use of AWS services" is also a correct answer.

INCORRECT: "Ensuring that AWS NTP servers are set to the correct time" is incorrect. Network Time Protocol (NTP) servers are an AWS responsibility.

INCORRECT: "Ensuring that access to data centers is restricted" is incorrect as this is security of the cloud and is an AWS responsibility.

INCORRECT: "Ensuring that hardware is disposed of properly" is incorrect as this is an AWS responsibility.

References:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

✓ What are the benefits of using IAM roles for applications that run on EC2 instances? (Select TWO.) *1/1

- ☒ More secure than storing access keys within applications ✓
- ☐ Role credentials are permanent
- ☐ Can apply multiple roles to a single instance
- ☐ Easier to configure than using storing access keys within the EC2 instance
- ☒ It is easier to manage IAM roles ✓

Feedback

Explanation

Using IAM roles instead of storing credentials within EC2 instances is more secure It is also easier to manage roles.

CORRECT: "More secure than storing access keys within applications" is the correct answer.

CORRECT: "It is easier to manage IAM roles" is the correct answer.

INCORRECT: "Easier to configure than using storing access keys within the EC2 instance" is incorrect. It is not easier to configure as there are extra steps that need to be completed.

INCORRECT: "Can apply multiple roles to a single instance" is incorrect. You cannot apply multiple roles to a single instance.

INCORRECT: "Role credentials are permanent" is incorrect. Role credentials are temporary, not permanent, and are rotated automatically.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

✓ What is the name for the top-level container used to hold objects within Amazon S3? *1/1

- ☐ Instance Store
- ☐ Folder
- ☒ Bucket
- ☐ Directory



Feedback

Explanation

Amazon S3 is an object-based storage system. You upload your objects into buckets.

CORRECT: "Bucket" is the correct answer.

INCORRECT: "Folder" is incorrect. Though S3 is a flat structure (not hierarchical), folders can be used for grouping objects. However, this is not the top-level container.

INCORRECT: "Directory" is incorrect. Directories are usually associated with filesystems rather than object-based storage systems.

INCORRECT: "Instance Store" is incorrect. An Instance Store is a type of ephemeral block-based storage service available to EC2 instances.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html#create-bucket-intro>

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/using-folders.html>

✓ What AWS service offers managed DDoS protection? *

1/1

- ☒ AWS Shield
- ☐ AWS Firewall Manager
- ☐ Amazon GuardDuty
- ☐ Amazon Inspector



Feedback

Explanation

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.

CORRECT: "AWS Shield" is the correct answer (as explained above.)

INCORRECT: "AWS Firewall Manager" is incorrect. AWS Firewall Manager is a security management service which allows you to centrally configure and manage firewall rules across your accounts and does not protect from DDoS attacks.

INCORRECT: "Amazon GuardDuty" is incorrect. Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation. It does not protect you from DDoS attacks.

INCORRECT: "Amazon Inspector" is incorrect also as Inspector is a fully managed vulnerability assessment tool and does not protect from DDoS attacks.

References:

<https://aws.amazon.com/shield/>

✓ Which of the below is an example of optimizing for cost? *

1/1

- ☐ Provision extra capacity to allow for growth
- ☐ Choosing the fastest EC2 instance to ensure performance
- ☒ Replace an EC2 compute instance with AWS Lambda
- ☐ Deploy resources with AWS CloudFormation



Feedback

Explanation

Where possible, you should replace EC2 workloads with AWS managed services that don't require you to take any capacity decisions. AWS Lambda is a serverless services and you only pay for actual processing time. Other examples of services that you don't need to make capacity decisions with include: ELB, CloudFront, SQS, Kinesis Firehose, SES, and CloudSearch.

CORRECT: "Replace an EC2 compute instance with AWS Lambda" is the correct answer.

INCORRECT: "Choosing the fastest EC2 instance to ensure performance" is incorrect. You should not choose the fastest EC2 instance if you're trying to optimize for cost as this will be expensive, you should right-size your EC2 instances, so you use the cheapest EC2 instance to suit your workload's requirements.

INCORRECT: "Provision extra capacity to allow for growth" is incorrect. Provisioning extra capacity for growth is not an example of cost optimization. With cloud computing you no longer need to do this as you can configure applications, databases and storage systems to grow on demand.

INCORRECT: "Deploy resources with AWS CloudFormation" is incorrect. Deploying resources with CloudFormation is great for consistently deploying application configurations from a template. However, this is not an example of cost optimization, it is more an example of operational optimization.

References:

<https://aws.amazon.com/aws-cost-management/>

✓ Which AWS service monitors AWS accounts continuously for malicious activity and unauthorized behavior? *1/1

- ☐ AWS Config
- ☐ Amazon Inspector
- ☒ Amazon GuardDuty
- ☐ Amazon Macie



Feedback

Explanation

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

CORRECT: "Amazon GuardDuty" is the correct answer (as explained above.)

INCORRECT: "Amazon Macie" is incorrect. Amazon Macie helps identify PII data within S3 Bucket and does not detect threats.

INCORRECT: "AWS Config" is incorrect. 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. It does not detect threats.

INCORRECT: "Amazon Inspector" is incorrect also as Inspector is a fully managed vulnerability assessment tool - it doesn't detect threat.

References:

<https://aws.amazon.com/guardduty/>

✓ Which of the following Amazon EC2 pricing models allows customers to use existing server-bound software licenses? *1/1

- ☒ Dedicated Hosts
- ☐ Spot Instances
- ☐ Reserved Instances
- ☐ On-Demand Instances



Feedback

Explanation

Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2, so that you get the flexibility and cost effectiveness of using your own licenses, but with the resiliency, simplicity and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirements.

CORRECT: "Dedicated Hosts" is the correct answer.

INCORRECT: "On-Demand Instances" is incorrect. This is a standard pricing model and does not offer the advantages requested.

INCORRECT: "Spot Instances" is incorrect. This is used to obtain discounted pricing for short-term requirements that can be interrupted.

INCORRECT: "Reserved Instances" is incorrect. This is used to lower cost by reserving usage of an instance for a term of 1 or 3 years.

References:

<https://aws.amazon.com/ec2/dedicated-hosts/>

✓ Which service can be used to manage configuration versions? *

1/1

- ☐ Amazon Inspector
- ☐ AWS Artifact
- ☒ AWS Config
- ☐ AWS Service Catalog



Feedback

Explanation

AWS Config is a fully-managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and regulatory compliance.

CORRECT: "AWS Config" is the correct answer.

INCORRECT: "AWS Service Catalog" is incorrect. AWS Service Catalog is used to create and manage catalogs of IT services that you have approved for use on AWS, including virtual machine images, servers, software, and databases to complete multi-tier application architectures.

INCORRECT: "AWS Artifact" is incorrect. AWS Artifact is a central resource for compliance-related information. This service can be used to get compliance information related to AWS' certifications/attestations.

INCORRECT: "Amazon Inspector" is incorrect. Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

References:

<https://docs.aws.amazon.com/config/latest/developerguide/how-does-config-work.html>

✓ When designing a VPC, what is the purpose of an Internet Gateway? * 1/1

- ☐ Provides Internet access for EC2 instances in private subnets
- ☒ Enables Internet communications for instances in public subnets ✓
- ☐ It's a bastion host for inbound management connections
- ☐ It's used for making VPN connections to a VPC

Feedback

Explanation

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

CORRECT: "Enables Internet communications for instances in public subnets" is the correct answer.

INCORRECT: "Provides Internet access for EC2 instances in private subnets" is incorrect. You cannot connect instances in a private subnet to the Internet using an Internet Gateway, you need a NAT Gateway or NAT Instance for this purpose.

INCORRECT: "It's a bastion host for inbound management connections" is incorrect. You cannot use an Internet Gateway as a bastion host, deploy an EC2 instance in a public subnet for this purpose.

INCORRECT: "It's used for making VPN connections to a VPC" is incorrect. You cannot use the Internet Gateway for making VPN connections to a VPC, you need a Virtual Private Gateway for this purpose.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

✓ Which of the following are NOT features of AWS IAM? (Select TWO.) * 1/1

- ☒ Charged for what you use
- ☐ Shared access to your AWS account
- ☐ Identity federation
- ☐ PCI DSS compliance
- ☒ Logon using local user accounts



Feedback

Explanation

You cannot use IAM to create local user accounts on any system. You are also not charged for what you use, IAM is free to use

The other options are all features of AWS IAM.

CORRECT: "Logon using local user accounts" is the correct answer.

CORRECT: "Charged for what you use" is the correct answer.

INCORRECT: "Shared access to your AWS account" is incorrect as explained above.

INCORRECT: "Identity federation" is incorrect as explained above.

INCORRECT: "PCI DSS compliance" is incorrect as explained above.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

✓ Which AWS service provides the ability to detect inadvertent data leaks of personally identifiable information (PII) and user credential data? *1/1

- ☒ Amazon Macie
- ☐ Amazon GuardDuty
- ☐ Amazon Inspector
- ☐ AWS Shield



Feedback

Explanation

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in Amazon S3.

Macie applies machine learning and pattern matching techniques to the Amazon S3 buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).

CORRECT: "Amazon Macie" is the correct answer.

INCORRECT: "Amazon GuardDuty" is incorrect. This is a service that analyzes your resources using anomaly detection and machine learning. It does not detect personally identifiable information.

INCORRECT: "Amazon Inspector" is incorrect. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. It does not detect personally identifiable information.

INCORRECT: "AWS Shield" is incorrect. This service is involved with protecting your resources of distributed denial of service (DDoS) attacks.

References:

<https://aws.amazon.com/macie/>

✓ Which AWS service lets connected devices easily and securely interact with cloud applications and other devices? *1/1

- ☐ AWS Server Migration Service (SMS)
- ☒ AWS IoT Core
- ☐ Amazon Workspaces
- ☐ AWS Directory Service



Feedback

Explanation

AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely.

CORRECT: "AWS IoT Core" is the correct answer.

INCORRECT: "AWS Directory Service" is incorrect. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud

INCORRECT: "Amazon Workspaces" is incorrect. Amazon WorkSpaces is a managed, secure cloud desktop service

INCORRECT: "AWS Server Migration Service (SMS)" is incorrect. AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for you to migrate thousands of on-premises workloads to AWS.

References:

<https://aws.amazon.com/iot-core/>

✓ Based on the shared responsibility model, which of the following security and compliance tasks is AWS responsible for? *1/1

- ☐ Updating operating systems
- ☒ Updating Amazon EC2 host firmware
- ☐ Granting access to individuals and services
- ☐ Encrypting data in transit



Feedback

Explanation

AWS are responsible for updating Amazon EC2 host firmware. This is considered "security of the cloud". All other tasks are the responsibility of the customer.

CORRECT: "Updating Amazon EC2 host firmware" is the correct answer.

INCORRECT: "Granting access to individuals and services" is incorrect. This is something a customer must perform to control access to the resources they use on AWS.

INCORRECT: "Encrypting data in transit" is incorrect. Encryption at rest and in-transit is a customer responsibility.

INCORRECT: "Updating operating systems" is incorrect. Customers are responsible for patching operating systems on Amazon EC2. AWS are only responsible for the host servers.

References:

<https://digitalcloud.training/certification-training/aws-certified-cloud-practitioner/aws-shared-responsibility-model/>

✗ Which support plan is the lowest cost option that allows unlimited cases to be open? *0/1

☒ Business

✗

☐ Basic

☐ Developer

☐ Enterprise

Correct answer

☒ Developer

Feedback

Explanation

With the Developer plan you can open unlimited cases. You can also open unlimited cases with the Business and Enterprise plans but these are more expensive. You cannot open any support cases with the basic support plan.

CORRECT: "Developer" is the correct answer.

INCORRECT: "Basic" is incorrect as explained above.

INCORRECT: "Business" is incorrect as explained above.

INCORRECT: "Enterprise" is incorrect as explained above.

References:

<https://aws.amazon.com/premiumsupport/plans/>

✓ How can a company configure automatic, asynchronous copying of objects in Amazon S3 buckets across regions? *1/1

- ☐ This is done by default by AWS
- ☒ Using cross-region replication ✓
- ☐ Using lifecycle actions
- ☐ By configuring multi-master replication

Feedback

Explanation

Cross-region replication (CRR) enables automatic, asynchronous copying of objects across buckets in different AWS Regions. Buckets configured for cross-region replication can be owned by the same AWS account or by different account

CORRECT: "Using cross-region replication" is the correct answer.

INCORRECT: "This is done by default by AWS" is incorrect as this is not true.

INCORRECT: "By configuring multi-master replication" is incorrect. Multi-master replication is not something you can do with Amazon S3 (Amazon Aurora has this feature).

INCORRECT: "Using lifecycle actions" is incorrect. Lifecycle actions cannot be configured to move to another storage class in a different region.

References:

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

✓ How can a company protect their Amazon S3 data from a regional disaster?

*1/1

- ☒ Use Cross-Region Replication (CRR) to copy to another region
- ☐ Enable Multi-Factor Authentication (MFA) delete
- ☐ Use lifecycle actions to move to another S3 storage class
- ☐ Archive to Amazon Glacier



Feedback

Explanation

Cross-Region replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions. The only option here that will help is to use CRR to copy the data to another region. This will provide disaster recovery.

CORRECT: "Use Cross-Region Replication (CRR) to copy to another region" is the correct answer.

INCORRECT: "Archive to Amazon Glacier" is incorrect. Moving to Glacier does not copy the data out of the region.

INCORRECT: "Use lifecycle actions to move to another S3 storage class" is incorrect as this will not move the data to another region.

INCORRECT: "Enable Multi-Factor Authentication (MFA) delete" is incorrect. Enabling MFA delete will not protect the data from a regional disaster.

References:

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

✓ Which AWS technology can be referred to as a “virtual hard disk in the cloud”? *1/1

- ☐ Amazon EFS Filesystem
- ☒ Amazon EBS volume
- ☐ Amazon S3 Bucket
- ☐ Amazon ENI



Feedback

Explanation

An Amazon Elastic Block Store (EBS) volume is often described as a “virtual hard disk in the cloud”. EBS volumes are block-level storage volumes that are attached to EC2 instances much as you would attach a virtual hard disk to a virtual machine in a virtual infrastructure.

CORRECT: “Amazon EBS volume” is the correct answer.

INCORRECT: “Amazon EFS Filesystem” is incorrect. An Amazon EFS filesystem is a file-level storage system that is accessed using the NFS protocol. Filesystems are mounted at the file, rather than the block level and are therefore not similar to a virtual hard disk.

INCORRECT: “Amazon S3 Bucket” is incorrect. Amazon S3 is an object-level storage service and is not mounted or attached. You use a REST API over HTTPS to access objects in an object store.

INCORRECT: “Amazon ENI” is incorrect. An Amazon Elastic Network Interface is a networking construct, not a storage construct.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes.html>

✓ Which of the following statements about AWS's pay-as-you-go pricing model is correct? *1/1

- ☐ It reduces operational expenditures
- ☒ It results in reduced capital expenditures ✓
- ☐ It is relevant only for Amazon EC2, Amazon S3, and Amazon DynamoDB
- ☐ It requires payment up front for AWS services

Feedback

Explanation

The pay-as-you-go pricing model means you only pay for the services and consumption you actually use. You are charged for compute, storage and outbound data transfer. This model reduces capital expenditure as you pay a monthly bill (operational expenditure).

CORRECT: "It results in reduced capital expenditures" is the correct answer.

INCORRECT: "It requires payment up front for AWS services" is incorrect. You can pay upfront for some services such as EC2 reserved instances to get better pricing but most services are offered on a consumption basis.

INCORRECT: "It is relevant only for Amazon EC2, Amazon S3, and Amazon DynamoDB" is incorrect. This is not true most AWS services are offered on a pay-as-you-go pricing model.

INCORRECT: "It reduces operational expenditures" is incorrect. This is not true, it reduces capital expenditures.

References:

<https://aws.amazon.com/pricing/>

✓ Which AWS service lets you add user sign up, sign-in and access control to web and mobile apps? *1/1

- ☐ AWS Directory Service
- ☐ AWS Artifact
- ☒ Amazon Cognito
- ☐ AWS CloudHSM



Feedback

Explanation

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0.

CORRECT: "AWS Cognito" is the correct answer.

INCORRECT: "AWS Artifact" is incorrect. AWS Artifact is your go-to, central resource for compliance-related information that matters to you.

INCORRECT: "AWS CloudHSM" is incorrect. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

INCORRECT: "AWS Directory Service" is incorrect. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

References:

<https://aws.amazon.com/cognito/>

✓ In which ways does AWS' pricing model benefit organizations? *

1/1

- ☐ Focus spend on capital expenditure, rather than operational expenditure
- ☐ Reduces the people cost of application development
- ☒ Reduce the cost of maintaining idle resources ✓
- ☐ Eliminates licensing costs

Feedback

Explanation

Using AWS you can provision only what you need and adjust resources automatically and elastically. This reduces the amount of resources that are sitting idle which reduces cost.

CORRECT: "Reduce the cost of maintaining idle resources" is the correct answer.

INCORRECT: "Eliminates licensing costs" is incorrect. AWS does not eliminate licensing costs or application development costs as you still need to licence and develop your application.

INCORRECT: "Focus spend on capital expenditure, rather than operational expenditure" is incorrect. AWS allows you to focus your spend on operational costs, not capital costs.

INCORRECT: "Reduces the people cost of application development" is incorrect as you still need people to develop applications.

References:

<https://aws.amazon.com/pricing/>

✗ Which actions are the responsibility of AWS, according to the AWS shared *0/1 responsibility model? (Select TWO.)

☒ Patching the operating system on Amazon EC2 instances



☐ Configuring security groups and network ACLs

☐ Enforcing a strict password policy for IAM users

☐ Patching the operating system on Amazon RDS instances

☒ Securing the virtualization layer



Correct answer

☒ Patching the operating system on Amazon RDS instances

☒ Securing the virtualization layer

Feedback

Explanation

Security of the virtualization layer comes down to the responsibility of AWS, as the AWS customer has no insight into this layer within the physical infrastructure.

Patching the operating system on Amazon RDS instances is AWS's responsibility as Amazon RDS is a managed service. As part of this, you do not need to manage or patch the operating system within the RDS database.

CORRECT: "Securing the virtualization layer" is the correct answer (as explained above.)

CORRECT: "Patching the operating system on Amazon RDS instances" is also a correct answer (as explained above.)

INCORRECT: "Patching the operating system on Amazon EC2 instances" is incorrect as EC2 is an Amazon EC2 instance is an Infrastructure as a Service tool, in which you simply have direct access to the underlying virtual machine. Therefore it is your responsibility to patch the operating system on any EC2 instance you use.

INCORRECT: "Enforcing a strict password policy for IAM users" is incorrect. It would be the responsibility of an AWS customer to regulate the password policy of IAM users.

INCORRECT: "Configuring security groups and network ACLs" is incorrect. It would be the responsibility of an AWS customer to configure security groups and network ACLs..

References:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

✓ You are evaluating AWS services that can assist with creating scalable application environments. Which of the statements below best describes the Elastic Load Balancer service? *1/1

- ☐ Helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application
- ☐ A highly available and scalable Domain Name System (DNS) service
- ☐ A network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS
- ☒ Automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses ✓

Feedback

Explanation

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses.

Elastic Load Balancing provides fault tolerance for applications by automatically balancing traffic across targets – Amazon EC2 instances, containers and IP addresses – and Availability Zones while ensuring only healthy targets receive traffic.

CORRECT: "Automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses" is the correct answer.

INCORRECT: "Helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application" is incorrect as this describes EC2 Auto Scaling.

INCORRECT: "A highly available and scalable Domain Name System (DNS) service" is incorrect as this describes Amazon Route 53.

INCORRECT: "A network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS" is incorrect as this describes AWS Direct Connect.

References:

<https://aws.amazon.com/elasticloadbalancing/>

✗ What do you need to log into the AWS console? *

0/1

- ☐ Key pair
- ☒ Access key and secret ID
- ☐ User name and password
- ☐ Certificate

✗

Correct answer

- ☒ User name and password

Feedback

Explanation

You can log into the AWS console using a user name and password. You cannot log in to the AWS console using a key pair, access key & secret ID or certificate.

CORRECT: "User name and password" is the correct answer.

INCORRECT: "Key pair" is incorrect as explained above.

INCORRECT: "Access key and secret ID" is incorrect as explained above.

INCORRECT: "Certificate" is incorrect as explained above.

References:

<https://aws.amazon.com/console/>

✓ Your organization has offices around the world and some employees travel between offices. How should their accounts be setup? *1/1

- ☐ Set the user account as a "global" account when created
- ☐ Enable MFA for the accounts
- ☒ IAM is a global service, just create the users in one place ✓
- ☐ Create a separate account in IAM within each region in which they will travel

Feedback

Explanation

IAM is a global service and all users that are created are able to login to the AWS Management Console from any location.

CORRECT: "IAM is a global service, just create the users in one place" is the correct answer.

INCORRECT: "Create a separate account in IAM within each region in which they will travel" is incorrect. You do not create separate IAM accounts in different regions as IAM is a global service.

INCORRECT: "Set the user account as a "global" account when created" is incorrect. There is no such thing as setting the account as "global".

INCORRECT: "Enable MFA for the accounts" is incorrect. Enabling multi-factor authentication is a good security practice but not necessary to enable users to travel to different locations.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_identity-management.html

✓ Which of the following is NOT a best practice for protecting the root user of an AWS account? *1/1

- ☐ Enable MFA
- ☐ Don't share the root user credentials
- ☐ Lock away the AWS root user access keys
- ☒ Remove administrative permissions



Feedback

Explanation

You cannot remove administrative permissions from the root user of an AWS account. Therefore, you must protect the account through creating a complex password, enabling MFA, locking away access keys (assuming they're even required), and not sharing the account details.

CORRECT: "Remove administrative permissions" is the correct answer.

INCORRECT: "Don't share the root user credentials" is incorrect as this is a best practice.

INCORRECT: "Enable MFA" is incorrect as this is a best practice.

INCORRECT: "Lock away the AWS root user access keys" is incorrect as this is a best practice.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

- ✓ A company is using the AWS CLI and programmatic access of AWS resources from its on-premises network.

*1/1

What is a mandatory requirement in this scenario?

- ☒ Using an AWS access key and a secret key
- ☐ Using an Amazon EC2 key pair
- ☐ Using Amazon API Gateway
- ☐ Using an AWS Direct Connect connection



Feedback

Explanation

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxrFcYEXAMPLEKEY). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests.

CORRECT: "Using an AWS access key and a secret key" is the correct answer.

INCORRECT: "Using an AWS Direct Connect connection" is incorrect. It is not a requirement that you use a Direct Connect connection. You can access public services via the API using the internet. For private services you can use Direct Connect, a VPN, or a bastion host.

INCORRECT: "Using Amazon API Gateway" is incorrect. You do not need API Gateway for programmatic access to the AWS API.

INCORRECT: "Using an Amazon EC2 key pair" is incorrect. A key pair is used to securely access EC2 resources and should not be confused with access keys.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

✓ Under the AWS Shared Responsibility Model, who is responsible for what? *1/1
(Select TWO.)

- ☐ Customers are responsible for edge locations
- ☐ Customers are responsible for compute infrastructure
- ☐ AWS are responsible for network and firewall configuration
- ☒ Customers are responsible for networking traffic protection ✓
- ☒ AWS are responsible for networking infrastructure ✓

Feedback

Explanation

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. Customers are responsible for security in the cloud and responsibilities vary by service.

Customers are responsible for networking traffic protection. This includes applying encryption and using security groups and Network ACLs.

AWS are responsible for networking infrastructure. The underlying networking equipment is maintained by AWS.

CORRECT: "Customers are responsible for networking traffic protection" is a correct answer.

CORRECT: "AWS are responsible for networking infrastructure" is also a correct answer.

INCORRECT: "Customers are responsible for compute infrastructure" is incorrect. AWS are responsible for compute infrastructure

INCORRECT: "AWS are responsible for network and firewall configuration" is incorrect. Customers are responsible for network and firewall configuration.

INCORRECT: "Customers are responsible for edge locations" is incorrect. AWS are responsible for edge locations.

References:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

✓ How does "elasticity" benefit an application design? *

1/1

- ☒ By automatically scaling resources based on demand ✓
- ☐ By reserving capacity to reduce cost
- ☐ By selecting the correct storage tier for your workload
- ☐ By reducing interdependencies between application components

Feedback

Explanation

Elasticity refers to the automatic scaling of resources based on demand. The benefit is that you provision only the necessary resources at a given time (optimizing cost) and don't have to worry about absorbing spikes in demand.

CORRECT: "By automatically scaling resources based on demand" is the correct answer.

INCORRECT: "By reducing interdependencies between application components" is incorrect. Elasticity does not reduce interdependencies between systems – this is known as loose coupling.

INCORRECT: "By selecting the correct storage tier for your workload" is incorrect. Selecting the correct storage tier would be an example of right-sizing, not elasticity.

INCORRECT: "By reserving capacity to reduce cost" is incorrect. Reserving capacity to reduce cost refers to using reservations such as EC2 Reserved Instances.

References:

<https://wa.aws.amazon.com/wat.concept.elasticity.en.html>

✓ In AWS IAM, what are the characteristics of users and groups? (Select TWO.) *1/1

- ☒ Groups can contain users only and cannot be nested. ✓
- ☐ Groups can be nested and can contain other groups.
- ☒ A user can be a member of multiple groups. ✓
- ☐ All new users are automatically added to a default group.
- ☐ A user can only be a member of a single group at one time.

Feedback

Explanation

In IAM, a user can be a member of multiple groups. One IAM user can be a part of a maximum of 5 groups. Also Groups are a flat hierarchy of users with similar permissions, and you cannot place a group within another group.

CORRECT: "A user can be a member of multiple groups" is the correct answer (as explained above.)

CORRECT: "Groups can contain users only and cannot be nested" is also a correct answer (as explained above.)

INCORRECT: "Groups can be nested and can contain other groups" is incorrect. This is also explained above.

INCORRECT: "A user can only be a member of a single group at one time" is incorrect. A user group can contain many users, and a user can belong to multiple user groups.

INCORRECT: "All new users are automatically added to a default group" is incorrect. Users do not have to be added to any group and can exist simply as users.

References:

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

✓ What is the most cost-effective Amazon S3 storage tier for data that is not often accessed but requires high availability? *1/1

- ☐ Amazon S3 One Zone-IA
- ☒ Amazon S3 Standard-IA
- ☐ Amazon S3 Standard
- ☐ Amazon Glacier



Feedback

Explanation

S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard with 99.9% availability

CORRECT: "Amazon S3 Standard-IA" is the correct answer.

INCORRECT: "Amazon S3 Standard" is incorrect as this class will cost more and is designed for data that requires regular access.

INCORRECT: "Amazon S3 One Zone-IA" is incorrect. S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and offers lower availability.

INCORRECT: "Amazon Glacier" is incorrect. Glacier is a data archiving solution so not suitable for a storage tier that requires infrequent access.

References:

<https://aws.amazon.com/s3/storage-classes/>

✓ Where are Amazon EBS snapshots stored? *

1/1

- ☐ Within the EBS block store
- ☐ On an Amazon EFS filesystem
- ☐ On an Amazon EBS instance store
- ☒ On Amazon S3



Feedback

Explanation

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.

CORRECT: "On Amazon S3" is the correct answer.

INCORRECT: "On an Amazon EBS instance store" is incorrect as explained above.

INCORRECT: "On an Amazon EFS filesystem" is incorrect as explained above.

INCORRECT: "Within the EBS block store" is incorrect as explained above.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

✓ What charges are applicable to Amazon S3 Standard storage class? *1/1
(Select TWO.)

☐ Retrieval fee

☒ Data egress ✓

☐ Data ingress

☐ Minimum capacity charge per object

☒ Per GB/month storage fee ✓

Feedback

Explanation

With the standard storage class you pay a per GB/month storage fee, and data transfer out of S3. Standard-IA and One Zone-IA have a minimum capacity charge per object. Standard-IA, One Zone-IA, and Glacier also have a retrieval fee. You don't pay for data into S3 under any storage class.

CORRECT: "Per GB/month storage fee" is the correct answer.

CORRECT: "Data egress" is the correct answer.

INCORRECT: "Retrieval fee" is incorrect as explained above.

INCORRECT: "Minimum capacity charge per object" is incorrect as explained above.

INCORRECT: "Data ingress" is incorrect as explained above.

References:

<https://aws.amazon.com/s3/pricing/>

✓ Which of the following acts as a virtual firewall at the Amazon EC2 instance level to control traffic for one or more instances? *1/1

- ☒ Security groups
- ☐ Virtual private gateways (VPG)
- ☐ Network Access Control Lists (ACL)
- ☐ Route table



Feedback

Explanation

A security group is an instance-level firewall that can be used to control traffic that reaches (ingress/inbound) and is sent out from (egress/outbound) your EC2 instances. Rules are created for inbound or outbound traffic. A security group can be attached to multiple EC2 instances.

CORRECT: "Security groups" is the correct answer.

INCORRECT: "Network Access Control Lists (ACL)" is incorrect as this is subnet-level firewall. You do not attach a Network ACL to an instance, you attach it to a subnet.

INCORRECT: "Virtual private gateways (VPG)" is incorrect. A VPG is the Amazon side of an AWS Managed VPN.

INCORRECT: "Route table" is incorrect as this is not a firewall but a table of routes for directing traffic between subnets within a VPC.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

✓ When an Amazon EC2 instance is stopped, which of the following AWS services can be used to identify the user who stopped it? *1/1

- ☐ VPC Flow Logs
- ☐ Amazon Inspector
- ☒ AWS CloudTrail
- ☐ Amazon CloudWatch



Feedback

Explanation

AWS CloudTrail tracks API calls that are made within a particular AWS account. It will track the API call made, the IP address it originated from and which IAM principal initiated the action and in this case will capture who stopped an EC2 instance.

CORRECT: "AWS CloudTrail" is the correct answer (as explained above.)

INCORRECT: "Amazon Inspector" is incorrect. Inspector is a fully managed vulnerability assessment tool and does not investigate who initiated any API call.

INCORRECT: "Amazon CloudWatch" is incorrect. Amazon CloudWatch is a monitoring and observability service which does not track API calls made within the account.

INCORRECT: "VPC Flow Logs" is incorrect. 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.

References:

<https://aws.amazon.com/cloudtrail/>

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

