Answer Sheet

Q1) A payments processing application is being deployed on a fleet of On-Demand EC2 instances in your VPC. The application has a lot of 3rd-party module dependencies which need to be downloaded first to the instance and then installed, for the application to run properly. You are required to improve the system to enable the instances to be deployed and be readily available to operate in the least amount of time possible.
Which of the following can help you accomplish this task?

○ Launch an OpsWorks stack which deploys the necessary EC2 instances and imports the payments processing application, including its required 3rd-party modules.
Explanation:-This option is incorrect.
○ Set up the User Data to install the application and the necessary 3rd-party modules on instance boot.
Explanation:-This option is incorrect.
✓ Create an AMI which contains the payments processing application and the necessary 3rd-party modules.
Explanation:-An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You must specify a source AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances when you need instances with different configurations.
An AMI includes the following:
* A template for the root volume for the instance (for ex
○ Use the cfn-init helper script in CloudFormation.
Explanation:-This option is incorrect.

Q2) You are building a face recognition system using AWS Deep Learning AMIs to train sophisticated, custom AI models and experiment with new algorithms. You tried to launch a new On-Demand EC2 instance to use a TensorFlow framework but you are always getting an InstanceLimitExceeded error message every time you do it.
As the SysOps Administrator, what is the reason for this error and how can you solve it?

✓ You have reached the limit on the number of instances that you can launch in a region. Request an instance limit increase on a per-region basis.
Explanation:-If you get an InstanceLimitExceeded error when you try to launch a new instance or restart a stopped instance, you have reached the limit on the number of instances that you can launch in a region. When you create your AWS account, AWS sets default limits on the number of instances you can run on a per-region basis.
To solve this issue, you can request an instance limit increase on a per-region basis.
○ You've reached your EBS volume limit. Submit a request to increase your Amazon EBS volume limit by completing the AWS Support Center Create Case form.
Explanation:-This option is incorrect because this describes the reason why your EC2 instance goes from the pending state to the terminated state immediately after restarting it.
○ AWS does not currently have enough available On-Demand capacity to service your request.
Explanation:-This option is incorrect because this describes the root cause of getting InsufficientInstanceCapacity error when you try to launch a new instance or restart a stopped instance.
○ The maximum limit of EC2 instances that you can launch in your Availability Zone (AZ) has been reached. Request an instance limit increase on a per-AZ basis.
Explanation:-This option is incorrect because you have reached the instance limit on the region and not on the Availability Zone.

Q3) A software development company has a suite of container-based applications on their on-premises data center which must be migrated to AWS. The applications need to be deployed on an infrastructure that automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.
Which of the following service should you use for this scenario?

○ None of these
Explanation:-This option is incorrect because aside from ECS or EKS, you can deploy your container-based application in Elastic Beanstalk.
○ AWS CloudFormation
Explanation:-This option is incorrect because CloudFormation is more suitable for creating and provisioning AWS infrastructure deployments predictably and repeatedly. It does not automatically handle the details of capacity provisioning, load balancing, scaling and many others unlike Elastic Beanstalk.
✓ AWS Elastic Beanstalk
Explanation:-Elastic Beanstalk supports the deployment of web applications from Docker containers. With Docker containers, you can define your own runtime environment. You can choose your own platform, programming language, and any application dependencies (such as package managers or tools), that aren't supported by other platforms. Docker containers are self-contained and include all the configuration information and software your web application requires to run. All environment variables defined in the El
○ AWS OpsWorks
Explanation:-This option is incorrect because OpsWorks is primarily used for configuration management and not for hosting application.

Q4) A SysOps Administrator has a fleet of EC2 instances inside an Auto Scaling Group and a couple of Lambda functions that are running inside the cloud infrastructure that she manages. Whenever she releases weekly updates of her code, inconsistencies occur due to not being able to manually update all relevant resources properly. Because of the large amount of resources present, she needs a way to group them together and deploy new versions of code consistently among the groups with minimal downtime.
Which among these services should she use to fix this issue?

○ Create OpsWorks recipes that will automatically launch resources containing the latest version of the code.
Explanation:-You could also use OpsWorks to deploy your code, however, this option is still incorrect because you don't need to launch new resources containing your new code when you can just update the ones that are already running.
✓ Use deployment groups in CodeDeploy to automate code deployments in a consistent manner.
Explanation:-CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda functions. It allows you to rapidly release new features, update Lambda function versions, avoid downtime during application deployment, and handle the complexity of updating your applications, without many of the risks associated with error-prone manual deployments.
○ Use CodeCommit to publish your code quickly in a private repository and push them to your resources for fast updates.
Explanation:-This option is incorrect as you mainly use CodeCommit for managing a source-control service that hosts private Git repositories. You

can store anything from code to binaries and work seamlessly with your existing Git-based tools. CodeCommit integrates with CodePipeline and CodeDeploy to streamline your development and release process.

- Create CloudFormation templates that have the latest configurations and code in them.

Explanation:-This option is incorrect since it is used for provisioning and managing stacks of AWS resources based on templates you create to model your infrastructure architecture. CloudFormation is recommended if you want a tool for granular control over the provisioning and management of your own infrastructure.

Q5) A medical startup is rushing to launch its AI-based medical diagnostics application. They urgently need to deploy their application to AWS where the capacity provisioning, load balancing, scaling, and application health monitoring can be handled automatically.
Which of the following AWS services will meet these requirements?

- ✅ AWS Elastic Beanstalk

Explanation:-With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

- Amazon ECS Cluster

Explanation:-This option is incorrect because an Amazon ECS Cluster is primarily used in deploying containerized applications which use Docker.

- Amazon EC2

Explanation:-This option is incorrect because you have to manually do all of the configuration, load balancing and provisioning in EC2 to meet the requirement which can be automatically handled if you use Elastic Beanstalk.

- Amazon EKS

Explanation:-This option is incorrect because Amazon EKS is primarily used in deploying containerized applications which use Kubernetes.

Q6)

Your company has an e-commerce website which uses images and other media files from an S3 bucket. The website is also hosted in AWS but it has a custom domain name (shop.tutorialsdojo.com) registered using Route 53.

There was a recent change in the bucket which hinders the website from showing the images hosted in S3.

Which of the following options should you do to fix this issue?

- ✅ Re-enable S3 CORS

Explanation:-Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS support, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.

- Re-enable S3 MFA Delete

Explanation:-This option is incorrect.

- Re-enable S3 bucket versioning

Explanation:-This option is incorrect.

- Re-enable S3 CRR

Explanation:-This option is incorrect.

Q7)

An innovative financial startup has been experiencing rapid growth and demand for their cloud-based services.

To meet the demand, they are planning to expand their cloud infrastructure for their online portal to two AWS regions: ca-central-1 Canada (Central) and ap-northeast-1 Asia Pacific (Tokyo) to serve their new clients. There is also a requirement to route more or less traffic to a given resource by specifying a value.

As their SysOps Administrator, how can you ensure that the traffic is served based on the geographic location of your users and your resources?

- Use the Route 53 service and create a new latency record for the website

Explanation:-This option is incorrect.

- Configure the load balancer of their online portal to redirect distant users to a closer region

Explanation:-This option is incorrect.

- Use a 3rd-party geolocation service to automatically route their users to the best-performing region.

Explanation:-This option is incorrect.

- ✅ Set up a Geoproximity routing using Route 53 to properly route their users to the best-performing region.

Explanation:-Geoproximity routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. You can also optionally choose to route more traffic or less to a given resource by specifying a value, known as a bias, that expands or shrinks the size of the geographic region from which traffic is routed to a resource.

Q8)

You are the Lead Systems Engineer of the IT Operations team in your company where you are creating CloudFormation stacks for all new applications that need to be deployed in your VPC.

There is one particular CloudFormation stack which is going to use a template to create a brand new VPC, EC2 Instances for your public web servers, an RDS database instance, and an Internet gateway.

Which of the following should you do to prevent any errors when deploying this stack?

- Verify that the UpdatePolicy attribute is added to the resources

Explanation:-This option is incorrect since the UpdatePolicy attribute is just used to specify how AWS CloudFormation handles updates to the

AWS::AutoScaling::AutoScalingGroup or AWS::Lambda::Alias resource.

Verify that the DeletionPolicy attribute is added to the resources.

Explanation:-This option is incorrect because the DeletionPolicy attribute is not required in this scenario and is used to preserve or backup a resource when its stack is deleted.

Verify that the CreationPolicy attribute is added to the resources.

Explanation:-This option is incorrect because the CreationPolicy attribute is just an optional for the CloudFormation stack to be properly deployed to AWS.

✅ Verify that the DependsOn attribute is added to the resources.

Explanation:-Take note that in this scenario, you are deploying a CloudFormation stack that creates a new VPC and an Internet Gateway. The DependsOn attribute is required if you have any VPC-gateway attachment in your stack.

Some resources in a VPC require a gateway (either an Internet or VPN gateway). If your AWS CloudFormation template defines a VPC, a gateway, and a gateway attachment, any resources that require the gateway are dependent on the gateway attachment. For example, an Amazon EC2 instance

---

Q9) A startup company is planning to host their innovative AI-based application on an EC2 instance which will be used by thousands of users around the globe. You need to design their architecture to speed up the distribution of their dynamic and static content to their global users.
Which of the following services can you use to implement this requirement?

AWS Lambda

Explanation:-This option is incorrect because AWS Lambda is a serverless computing service.

AWS SQS

Explanation:-This option is incorrect because AWS SQS is a queue service.

AWS SNS

Explanation:-This option is incorrect because AWS SNS is a notification service.

✅ AWS CloudFront

Explanation:-Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Q10) A software development company has developed a web application based on Docker containers, which they need to migrate over to their VPC. As the Senior Systems Administrator, you are responsible in ensuring that there are no maintenance overheads incurred in the deployment.
Which of the following would you use for this purpose?

Amazon Lambda

Explanation:- This option is incorrect because Amazon Lambda is primarily used for serverless computing and not for hosting containers such as Docker or Kubernetes.

Amazon EKS

Explanation:-This option is incorrect because Amazon EKS is used for hosting Kubernetes and not Docker.

Amazon EC2

Explanation:-This option is incorrect because using an EC2 instance means that you have to manage the underlying resources of your Docker application.

✅ Amazon ECS

Explanation:-Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container orchestration service that supports Docker containers and allows you to easily run and scale containerized applications on AWS. Amazon ECS eliminates the need for you to install and operate your own container orchestration software, manage and scale a cluster of virtual machines, or schedule containers on those virtual machines.

Q11) A commercial bank has recently adopted a hybrid cloud architecture which prompted them to migrate most of their applications to AWS. You are creating multiple CloudFormation stacks for all of the applications that will be used by different departments. You are tasked to ensure that all RDS database instances that you deploy should be kept even if the stack is deleted.
How can you satisfy this requirement?

Set the DeletionPolicy attribute for the stack resource to false

Explanation:-This option is incorrect.

Set the DeletionPolicy attribute for the stack resource to Snapshot

Explanation:-This option is incorrect.

✅ Set the DeletionPolicy attribute for the stack resource to Retain

Explanation:-With the DeletionPolicy attribute you can preserve or (in some cases) backup a resource when its stack is deleted. You specify a DeletionPolicy attribute for each resource that you want to control. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default.

DeletionPolicy Options:

-Delete: The AWS CloudFormation service deletes the resource and all its content if applicable during stack deletion. You can add this deletion policy to any resourc

Enable termination protection of the stack

Explanation:-This option is incorrect.

Q12)

You are working as a SysOps Administrator in a FinTech startup which develops an AI-based application that uses a NoSQL database. The application must be hosted on a large EC2 instance in AWS.

Which of the following would need to be implemented as part of this deployment?

Attach an IAM Role to the Amazon Aurora database to access the EC2 Instance.

Explanation:-This option is incorrect because Amazon Aurora is not a NoSQL database. You should use DynamoDB instead.

Attach an IAM Role to the DynamoDB database to access the EC2 Instance

Explanation:-This option is incorrect because you should attach the IAM role on the EC2 instance instead and not on the DynamoDB database since the instance will be the one that will send API requests. It should be the other way around.

Attach an IAM Role to the EC2 Instance to access Amazon Aurora database.

Explanation:-This option is incorrect because Amazon Aurora is not a NoSQL database. You should use DynamoDB instead.

Attach an IAM Role to the EC2 Instance to access DynamoDB.

Explanation:-In this scenario, you have to launch a NoSQL database for the application which is why you need to use DynamoDB. You also need to grant an IAM Role to the EC2 instance to access the DynamoDB database.

Applications that run on an EC2 instance must include AWS credentials in their AWS API requests. You could have your developers store AWS credentials directly within the EC2 instance and allow applications in that instance to use those credentials. But developers would then have to manage the

---

Q13) A multi-tier application, which is used internally by a financial services firm, is hosted on 2 On-Demand EC2 instances for its web and database tiers. You are required to ensure that these two instances can communicate with each other and ensure that the instances cannot communicate to the public Internet.
Which of the following options is the correct way of implementing this architecture?

Deploy the web and database layer on public subnets in separate AWS regions.

Explanation:-This option is incorrect because the instances would not be able to communicate between two regions unless you establish a connection between their VPCs

Deploy the web and database layer on private subnets in separate AWS regions.

Explanation:-This option is incorrect because the instances would not be able to communicate between two regions unless you establish a connection between their VPCs

Deploy the web and database layer on public subnets in a single AWS region.

Explanation:-This option is incorrect because public subnet will allow the instances to connect to the Internet, which is prohibited in the scenario.

Deploy the web and database layer on private subnets in a single AWS region.

Explanation:-Since the application is used internally in the company, you should deploy the web and database layer on a private subnet on the same AWS region. If the two instances are hosted in a different region, then these would not be able to communicate unless you establish a connection between the VPCs.

Q14) An employee creates a VPC to test his prototype application in AWS. After creating a VPC with a public subnet, he starts up an EC2 instance and deploys his application into it. When he has finished performing all the checks and tests, he stops his instance and proceeds to delete the created VPC using the VPC console.
Which of the following will happen next in this scenario?

The VPC will be deleted along with all resources attached to it.

Explanation:-This option is incorrect.

The VPC will be deleted and the EC2 instance will be automatically transferred to the default VPC.

Explanation:-This option is incorrect.

The VPC won't be deleted because there are still instances in it that haven't been terminated

Explanation:-You can delete your VPC at any time. However, you must terminate all instances in the VPC first. When you delete a VPC using the VPC console, AWS deletes all its components, such as subnets, security groups, network ACLs, route tables, Internet gateways, VPC peering connections, and DHCP options. When you delete a VPC using the command line, you must first terminate all instances, delete all subnets, custom security groups, and custom route tables, and detach any Internet gateway in the VPC.

The VPC won't be deleted until he deletes the public subnet first.

Explanation:-This option is incorrect.

Q15) One of the Big 4 accounting firms has recently hired you as their new IT Consultant. You are instructed to build a hybrid cloud architecture and satisfy regulatory requirements requiring the use of private connectivity between your on-premises network to AWS.
Which of the following services will allow you to connect your internal corporate network to your VPC without having to pass through the public Internet?

AWS S3 - Transfer Acceleration

Explanation:-This option is incorrect.

AWS Storage Gateway

Explanation:-This option is incorrect.

AWS Direct Connect

Explanation:-AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to public AWS services or to Amazon VPC, bypassing Internet service providers in your network path.

AWS Storage Gateway is incorrect because you are building a hybrid environment that needs a private, de

AWS Data Pipeline

Explanation:-This option is incorrect.

Q16) You are planning to migrate an application server from your on-premises network to AWS. The server should be deployed in a private subnet and should also be able to access an S3 bucket without traversing the Internet. For security purposes, the traffic between your VPC and S3 should not leave the Amazon network.
Which of the following VPC components should you integrate in your architecture?

VPC Endpoint

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

Endpoints are virtual devices. They are horizontally scaled, redundant, and h

Egress-Only Internet Gateways

Explanation:-This option is incorrect.

NAT Gateway
Explanation:-This option is incorrect.
Internet Gateway
Explanation:-This option is incorrect.

Q17) You are setting up a Wordpress website on two On-Demand EC2 instances which are deployed on a public subnet and for its database tier, you are using a MySQL database in RDS which is in a private subnet. During the initial testing, you noticed that the web servers could not establish communication with your RDS instance.
Which of the following should you do to fix this connectivity issue?

Check that an Elastic IP is assigned to the database server.
Explanation:-This option is incorrect because the communication needs to be done via the private IP address and not on a public address, hence, an Elastic IP is not necessary.
Check that the main route table has the required routing that connects the public subnet to the private subnet where the RDS instance is.
Explanation:-This option is incorrect because the subnets within a VPC can already connect with one another and, hence, this statement is incorrect.
✅ Check that the security group for the database server is allowing the required inbound communication from the EC2 instance.
Explanation:-Security groups control the access that traffic has in and out of a DB instance. Three types of security groups are used with Amazon RDS: DB security groups, VPC security groups, and Amazon EC2 security groups. In simple terms, these work as follows:
• A DB security group controls access to EC2-Classic DB instances that are not in a VPC.
• A VPC security group controls access to DB instances and EC2 instances inside a VPC.
• An EC2 security group controls access to an EC2 i
Check that the Internet gateway is attached to the VPC.
Explanation:-This option is incorrect because the scenario did not state that the web servers could not access the Internet, hence, an Internet Gateway is not the root cause of the issue.

Q18) You are working for a large insurance firm which just recently decided to use AWS. One of your fellow Systems Administrators has defined the following inbound NACL rules for a subnet:
Refer Image
An inbound rule has also been defined on the Security Group applied to an EC2 instance on this subnet to allow incoming traffic to port 80 from anywhere. In this scenario, which of the following is true based on these settings?

All traffic going out of the subnet will be denied.
Explanation:-This option is incorrect because the question only states inbound rules. We don't know the outbound rules to make a decision on this statement but by default, NACL and Security groups will allow outbound connections.
There will be an error in setting the rules for the Security Group rules due to the conflict in inbound rules.
Explanation:-This option is incorrect because the settings for the NACL and the Security Groups are separate. You won't receive any error from AWS when you do this.
✅ All traffic on all ports will not be allowed to flow into the subnet.
Explanation:-This option is the correct answer. In the above screenshot, the Rule number 100 will be evaluated first and therefore all traffic will be denied into the subnet. NACL will apply this to the whole subnet, and not just for a single instance.
An HTTP port 80 request from a workstation on the Internet with IP address 52.78.19.20 will be allowed onto the EC2 instance.
Explanation:-This option is incorrect because by default, Rule 100 will be evaluated, thus, any incoming traffic will be denied.

Q19) A company has a fleet of On-Demand EC2 instances on their new VPC created using the AWS CLI. You noticed that all recently launched EC2 instances do not have public DNS hostnames. This prevents you from accessing the instances over the Internet.
Which of the following could be a possible reason for this issue?

By default, the enableDnsSupport is set to false and enableDnsHostNames is set to true for VPCs created using the AWS CLI
Explanation:-This option is incorrect.
By default, both the enableDnsSupport and enableDnsHostNames are set to false for VPCs created using the AWS CLI
Explanation:-This option is incorrect.
✅ By default, the enableDnsHostNames is set to false for VPCs created using the AWS CLI
Explanation:-Domain Name System (DNS) is a standard by which names used on the Internet are resolved to their corresponding IP addresses. A DNS hostname is a name that uniquely and absolutely names a computer; it's composed of a host name and a domain name. DNS servers resolve DNS hostnames to their corresponding IP addresses.
Public IPv4 addresses enable communication over the Internet, while private IPv4 addresses enable communication within the network of the instance (either EC2-Classic or a VPC). Y
By default, the enableDnsSupport is set to false for VPCs created using the AWS CLI
Explanation:-This option is incorrect.

Q20) An aerospace engineering company wants to establish a hybrid cloud architecture that connects their on-premises corporate data centre to their Virtual Private Cloud hosted in AWS. Most of their mission-critical systems are still hosted on their on-premises network so they just need a cost-effective connection to their VPC.
Which of the following should you use in implementing the hybrid architecture?

AWS Direct Connect Gateway
Explanation:-This option is incorrect because a Direct Connect connection is much more expensive than a VPN connection. This should only be considered for low latency connections and when you are willing to bear the high cost of an AWS Direct Connect connection.
AWS Direct Connect
Explanation:-This option is incorrect because a Direct Connect connection is much more expensive than a VPN connection. This should only be considered for low latency connections and when you are willing to bear the high cost of an AWS Direct Connect connection.
AWS VPC Peering
Explanation:-This option is incorrect because a VPC peering connection is just used to connect two or more VPCs.
✅ AWS VPN Managed Connections
Explanation:-By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection. Although the term VPN connection is a general term, a VPN connection in AWS refers to the

connection between your VPC and your own network. AWS supports Internet Protocol s

Q21) An investment bank is storing the account transactions of their clients in S3. As the SysOps Administrator of the company, you enabled Versioning and MFA Delete to secure the objects stored in the S3 bucket from accidental deletion.
In this scenario, which of the following operations in S3 will now require additional authentication? (Choose 2)

- Renaming an object.

Explanation:-This option is incorrect.

- Moving an object.

Explanation:-This option is incorrect.

- ✅ Change the versioning state of your bucket.

Explanation:-You can optionally add another layer of security by configuring a bucket to enable MFA (multi-factor authentication) Delete, which requires additional authentication for either of the following operations:
• Change the versioning state of your bucket
• Permanently delete an object version
MFA Delete requires two forms of authentication together:
• Your security credentials
• The concatenation of a valid serial number, a space, and the six-digit code displayed on

- ✅ Permanently deleting an object version.

Explanation:-You can optionally add another layer of security by configuring a bucket to enable MFA (multi-factor authentication) Delete, which requires additional authentication for either of the following operations:
• Change the versioning state of your bucket
• Permanently delete an object version
MFA Delete requires two forms of authentication together:
• Your security credentials
• The concatenation of a valid serial number, a space, and the six-digit code displayed on

- Change the ACL of your bucket.
- Enabling CORS in the bucket.

Q22) You are working as a SysOps Administrator for a leading commercial bank which is currently implementing a hybrid cloud architecture. There is a requirement to use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. The objective is to minimize the need to scale your on-premises storage infrastructure while still providing your applications with low-latency access to their frequently accessed data.
Which type of AWS Storage Gateway is best to use for this scenario?

- Stored Volume Gateway

Explanation:-This option is incorrect.

- ✅ Cached Volume Gateway

Explanation:-By using cached volumes, you can use Amazon S3 as your primary data storage while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you wri

- File Gateway

Explanation:-This option is incorrect.

- Virtual Tape Library (VTL)

Explanation:-This option is incorrect.

Q23) You are deploying a critical business application in AWS which uses MongoDB and an Amazon ECS cluster. For the database-tier, you have to launch MongoDB on a large EC2 instance with attached EBS volumes to handle large workloads.
Which of the following EBS volume type would you use for the EBS volumes of the underlying EC2 instance?

- Throughput Optimized HDD

Explanation:-This option is incorrect.

- ✅ Provisioned IOPS SSD

Explanation:-Provisioned IOPS SSD is a high-performance SSD volume for mission-critical low-latency or high-throughput workloads. This is suitable for critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume and for large database workloads which uses MongoDB, Cassandra, Microsoft SQL Server etc.

- General Purpose SSD

Explanation:-This option is incorrect.

- Cold HDD

Explanation:-This option is incorrect.

Q24) A digital marketing company has a proprietary enterprise application that is hosted on an Auto Scaling group of On-Demand EC2 instances. It needs to have a durable, high throughput data storage for their content management system and should provide parallel shared access to their servers.
Which of the following would be the suitable data store for the fleet of EC2 instances?

- Provisioned IOPS EBS Volumes

Explanation:-This option is incorrect because EBS volumes are mainly used for local block level storage for EC2 Instances. Although they can provide a high throughput for an EC2 instance, they cannot provide parallel access to multiple instances, which is required in the question.

- Throughput Optimized EBS Volumes

Explanation:-This option is incorrect because EBS volumes are mainly used for local block level storage for EC2 Instances. Although they can provide a high throughput for an EC2 instance, they cannot provide parallel access to multiple instances, which is required in the question.

- S3

Explanation:-This option is incorrect because S3 is primarily used for object level storage that is available from the Internet.

- ✅ EFS

Explanation:-Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It is easy to use and offers a simple interface that allows you to create and configure file systems quickly and easily. Amazon EFS is built to elastically scale on demand without disrupting applications, growing and shrinking automatically as you add and remove files, so your

applications have the storage they need, when they need it.
It is desi

Q25) You are working as a Systems Administrator for a multinational investment bank where you are instructed to set up a Multi-AZ RDS database with Read Replicas configured to other AWS regions. The database will be used by a web application hosted on a Reserved EC2 instance. You are getting an error whenever you try to connect the application to the RDS database.
Which of the following is a potential cause for this issue? (Choose 3)

- The ingress and egress rules of the Network ACL, which allows traffic to the DB instance, are not properly added.

Explanation:-This option is incorrect.

- ✅ The ingress and egress rules of the security group, which allows traffic to the DB instance, are not properly added.

Explanation:-When you cannot connect to a DB instance, the following are common causes:
• The access rules enforced by your local firewall and the ingress IP addresses that you authorized to access your DB instance in the instance's security group are not in sync. The problem is most likely the ingress rules in your security group. By default, DB instances do not allow access; access is granted through a security group. To grant access, you must create your own security group with specific ingress an

- ✅ Your DB instance is still being created and is not yet available. Depending on the size of your DB instance, it can take up to 20 minutes before an instance becomes available.

Explanation:-When you cannot connect to a DB instance, the following are common causes:
• The access rules enforced by your local firewall and the ingress IP addresses that you authorized to access your DB instance in the instance's security group are not in sync. The problem is most likely the ingress rules in your security group. By default, DB instances do not allow access; access is granted through a security group. To grant access, you must create your own security group with specific ingress an

- The Enhanced Networking feature is not enabled in the EC2 instance.

Explanation:-This option is incorrect.

- The SSL certificate used by the EC2 instance is not supported by RDS.

Explanation:-This option is incorrect.

- ✅ The port you specified when you created the DB instance cannot be used to send or receive communications due to your local firewall restrictions.

Explanation:-When you cannot connect to a DB instance, the following are common causes:
• The access rules enforced by your local firewall and the ingress IP addresses that you authorized to access your DB instance in the instance's security group are not in sync. The problem is most likely the ingress rules in your security group. By default, DB instances do not allow access; access is granted through a security group. To grant access, you must create your own security group with specific ingress an

---

Q26) A data analytics company decided to augment their on-premises infrastructure with AWS. They need a new service that can analyze clickstream data from their global clients in order to segment users, understand user preferences, and deliver more effective ads. As the SysOps Administrator, you have to set up their cloud architecture where it can automatically provision thousands of compute instances to process data at any scale.
Which of the following should you use to meet the requirement?

- Amazon ElastiCache.

Explanation:-This option is incorrect.

- ✅ Amazon Elastic MapReduce.

Explanation:-Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. It utilizes a hosted Hadoop framework running on the web-scale infrastructure of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3). With Amazon EMR, you can provision one, hundreds, or thousands of compute instances to process data at any scale.
You can easily increase or decrease the number of inst

- Amazon Relational Database Service.

Explanation:-This option is incorrect.

- Amazon DynamoDB.

Explanation:-This option is incorrect.

Q27) You are working in a leading global investment bank which has strict security compliance requirements in handling their financial data. As the SysOps Administrator, you are instructed to ensure that the data stored in the EBS Volumes, which are used by your EC2 instances, are also available in another AWS region. This will provide a better redundancy to critical data stored in the volumes.
How can you achieve this?

- Use the Amazon Data Lifecycle Manager (DLM) for EBS Snapshots

Explanation:-This option is incorrect because although the Amazon Data Lifecycle Manager (DLM) for EBS Snapshots provides a simple, automated way to back up data stored on Amazon EBS volumes, it does not have the capability to create a snapshot and automatically move it to another region. You still have to copy the snapshot and move it to another region.

- Create a copy of the EBS volumes in the new region.

Explanation:-This option is incorrect because you have to copy a snapshot of the actual EBS volume and move it to another region.

- Create a snapshot from the EBS volumes in another region

Explanation:-This option is incorrect because you cannot directly create a snapshot in another region.

- ✅ Create a snapshot of the volume and then copy it to the new region.

Explanation:-With Amazon EBS, you can create point-in-time snapshots of volumes, which we store for you in Amazon S3. After you've created a snapshot and it has finished copying to Amazon S3 (when the snapshot status is completed), you can copy it from one AWS region to another, or within the same region. Amazon S3 server-side encryption (256-bit AES) protects a snapshot's data in-transit during a copy operation. The snapshot copy receives an ID that is different than the ID of the original snapshot.

Q28) A company has been using a legacy Virtual Tape Library system in their on-premises data center which still uses a manual tape management process. The retrieval time of the tape is slow and you were instructed to overhaul the system and use AWS to streamline the backup processes, reduce the manual effort, and gain predictable retrieval times.
Which of the following is the most suitable service to use in this scenario?

- Store the tape data directly to an Amazon S3 bucket.

Explanation:-This option is incorrect because S3 in itself does not automatically allow you to store and retrieve objects using industry-standard file protocols such as Network File System (NFS) and Server Message Block (SMB).

Use Cold HDD EBS Volumes to store the tape data.
Explanation:-This option is incorrect because EBS volumes is used for local storage for EC2 Instances.
Set up a tape gateway using AWS Storage Gateway.
Explanation:-AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. You can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration. Your applications connect to the service through a virtual machine or hardware gateway appliance using standard storage protocols, such as NFS, SMB and iSCSI. The gateway connects to AWS storage services, such as Amazon S3, Amazon Glacier, and Amaz
Use Amazon Glacier to store the tape data in the most cost-effective manner.
Explanation:-This option is incorrect because even though Glacier is used for archiving data, when storing tape data, it is better to use the AWS Storage Gateway service.

Q29) A media company is heavily using various AWS cloud resources for their daily operations. Your manager wants to get the utilization of these resources and be able to know which areas of their cloud architecture they can optimize to save on costs. Which of the following services can be used for this purpose?

AWS CloudTrail
Explanation:-This option is incorrect because AWS CloudTrail is used for API logging.
AWS Inspector
Explanation:-This option is incorrect because AWS Inspector is primarily used to check the server for vulnerabilities and not provide utilization and cost reports.
AWS Cost and Usage reports
Explanation:-The AWS Cost and Usage report tracks your AWS usage and provides estimated charges associated with your AWS account. The report contains line items for each unique combination of AWS product, usage type, and operation that your AWS account uses. You can customize the AWS Cost and Usage report to aggregate the information either by the hour or by the day.
AWS Config
Explanation:-This option is incorrect because AWS Config is just a configuration service and does not provide any cost and usage information for your VPC.

Q30) Your supervisor wants to have detailed information on the performance metrics of the AWS resources which are being used to host the company website. You know that by using CloudWatch agent, it enables you to collect more logs and provide more details on your systems, however, you are also aware of its limitations.
Which of these functions is not available with CloudWatch agent?

Collect more system-level metrics from Amazon EC2 instances, including in-guest metrics, in addition to the metrics for EC2 instances.
Explanation:-This option is incorrect.
Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS
Explanation:-This option is incorrect.
Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows Server.
Explanation:-This option is incorrect.
Collect information on vulnerabilities and errors that are present in your system and create a report based on the findings of the agent.
Explanation:-The unified CloudWatch agent enables you to do the following:
1. Collect more system-level metrics from Amazon EC2 instances, including in-guest metrics, in addition to the metrics for EC2 instances. The additional metrics are listed in Metrics Collected by the CloudWatch Agent.
2. Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS.
3. Collect logs from Amazon EC2 instances and on-p

Q31)

A data warehouse is hosted on a Redshift cluster which is being used by an online analytics application in your AWS VPC. There is a requirement to ensure that the logs for the cluster are tracked and stored for auditing purposes, which is done annually.

The logs should contain the information about connections and user activities in your database.

Which of the following logs would be available for you to track your Redshift cluster? (Choose 3)

User activity log
Explanation:-Amazon Redshift logs information about connections and user activities in your database. These logs help you to monitor the database for security and troubleshooting purposes, which is a process often referred to as database auditing. The logs are stored in the Amazon Simple Storage Service (Amazon S3) buckets for convenient access with data security features for users who are responsible for monitoring activities in the database. Amazon Redshift logs information in the following log files:
User log
Explanation:-Amazon Redshift logs information about connections and user activities in your database. These logs help you to monitor the database for security and troubleshooting purposes, which is a process often referred to as database auditing. The logs are stored in the Amazon Simple Storage Service (Amazon S3) buckets for convenient access with data security features for users who are responsible for monitoring activities in the database. Amazon Redshift logs information in the following log files:
ELB access logs
Explanation:-This option is incorrect.
CloudTrail logs
Explanation:-This option is incorrect.
CloudWatch logs
Explanation:-This option is incorrect.
Connection log
Explanation:-Amazon Redshift logs information about connections and user activities in your database. These logs help you to monitor the database for security and troubleshooting purposes, which is a process often referred to as database auditing. The logs are stored in the Amazon Simple Storage Service (Amazon S3) buckets for convenient access with data security features for users who are responsible for monitoring activities in the database.

Amazon Redshift logs information in the following log files:

Q32)

An accounting company has recently adopted a hybrid cloud infrastructure and they instructed you to set up a system to store each of their employee's work files to an S3 bucket. You noticed most documents which are created after 3 months are no longer accessed by the users.

As the company's Systems Administrator, which of the following is the most suitable way to reduce the storage costs while still providing the users access to the files?

- Set up a lifecycle policy to automatically move files older than 3 months to S3 One Zone-Infrequent Access.

Explanation:-This option is incorrect because Glacier is a more cost-efficient storage option compared with other S3 storage classes.

- ✅ Set up a lifecycle policy that automatically move files older than 3 months to Glacier.

Explanation:-To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle configuration which 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 STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage

- Enable S3 Versioning and MFA.

Explanation:-This option is incorrect because versioning and MFA are primarily used to ensure objects are not accidentally deleted.

- Set up an S3 bucket policy to only allow access to objects that are created less than 3 months ago.

Explanation:-This option is incorrect because the bucket policy is used for permission access.

Q33)

You are migrating an online accounting application to AWS which uses TCP protocol.

As the Systems Administrator, you are instructed to improve the scalability and availability of the application and to ensure that the IP address of the clients using the application are recorded for tracking.

Which of the following steps would you implement to fulfil this requirement?

- Use Route 53 with Weighted Routing to distribute load on two application servers in different Availability Zones.

Explanation:-This option is incorrect because Weighted Routing does not provide the IP address of the clients.

- Use Route 53 with Latency Based Routing enabled to distribute load on two or more application servers in different Availability Zones.

Explanation:-This option is incorrect because Route 53 latency based routing does not provide the IP address of the clients.

- Use an ELB with a TCP Listener and Cross-Zone Load Balancing enabled to load-balance the two application servers located in different Availability Zones.

Explanation:-This option is incorrect because although implementing cross-zone load balancing provides high availability, it will not be able to provide the IP address of the clients.

- ✅ Use an Elastic Load Balancer with a TCP Listener then enable the Proxy Protocol to distribute load on two or more application servers in different AZs.

Explanation:-Proxy Protocol is an Internet protocol used to carry connection information from the source requesting the connection to the destination for which the connection was requested. Elastic Load Balancing uses Proxy Protocol version 1, which uses a human-readable header format.
By default, when you use Transmission Control Protocol (TCP) for both front-end and back-end connections, your Classic Load Balancer forwards requests to the instances without modifying the request headers. If you enable

---

Q34) A startup is using AWS to host their cloud-based traffic solutions. They need to publish their custom metrics from several smart devices of a road traffic control system to CloudWatch for proper monitoring. To provide better surveillance, there is a requirement to publish the metrics at an interval of 1 second.
Which of the following options will allow you to accomplish this? (Choose 2)

- Go to CloudWatch dashboard and enable per second monitoring of your metrics.

Explanation:-This option is incorrect because you need to publish a new custom metric at high resolution. There is no option to just enable a per-second metric monitoring.

- Set up another CloudWatch account with detailed monitoring to enable per second monitoring.

Explanation:-This option is incorrect because you don’t need to set up another CloudWatch account to do this.

- Publish metrics with standard resolution which has a data granularity of one second.

Explanation:-This option is incorrect because you need high resolution for 1 second based metrics.

- ✅ Publish metrics with high resolution which has a data granularity of one second

Explanation:-Option 4 is correct. Metrics produced by AWS services are standard resolution by default. When you publish a custom metric, you can define it as either standard resolution or high resolution. When you publish a high-resolution metric, CloudWatch stores it with a resolution of 1 second, and you can read and retrieve it with a period of 1 second, 5 seconds, 10 seconds, 30 seconds, or any multiple of 60 seconds.

- Publish custom metrics from the AWS Console.

Explanation:-This option is incorrect because you cannot publish custom metrics from the Console.

- ✅ Use the AWS CLI to publish custom metrics

Explanation:-This option is correct because you need to create a custom metric for this scenario. You need to use the AWS CLI to publish the custom metrics since AWS doesn’t let you publish custom metrics from the Console.

Q35) A legacy application is using a Classic Load Balancer in AWS which routes each request independently to the registered EC2 instance with the smallest load. You enabled the sticky session feature to allow the load balancer to bind a user's session to a specific EC2 instance.
What is the name of the cookie that the load balancer creates, which is used to map the user's session?

- sticky-session-id

Explanation:-This option is incorrect.

- aws-sticky-session-id

Explanation:-This option is incorrect.

SESSION-ELB

Explanation:-This option is incorrect.

AWSELB

Explanation:-By default, a Classic Load Balancer routes each request independently to the registered instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance.

The key to managing sticky sessions is to determine how long your load balancer should consistently route the user's

---

Q36) A company has hundreds of Customer Master Keys (CMKs) which they are using with the Amazon Key Management Service to secure their S3 buckets, RDS instances, and other AWS resources. You were instructed to delete some CMKs to avoid management overhead and costs associated with maintaining unused keys.
In this scenario, which of the following is true regarding the deletion of customer master keys? (Choose 2)

A CMK that is pending deletion cannot be used in any cryptographic operation.

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

A CMK that is pending deletion can still be used in any cryptographic operation.

Explanation:-This option is incorrect because a CMK that is pending deletion cannot be used in any cryptographic operation. Option 4 is incorrect because a CMK that is pending deletion cannot be used in any cryptographic operation.

AWS KMS does not rotate the backing keys of CMKs that are pending deletion.

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

AWS KMS still rotates the backing keys of CMKs that are pending deletion.

Explanation:-This option is incorrect because AWS KMS does not rotate the backing keys of CMKs that are pending deletion.

You can directly delete a CMK immediately.

Explanation:-This option is incorrect because you cannot directly delete a CMK immediately. You have to schedule its deletion.

You can schedule the CMK for deletion with a default waiting period of 7 days.

Explanation:-This option is incorrect because although you can schedule the CMK for deletion, its default waiting period is 30 days and not 7 days.

Q37) You have a legacy web application which is hosted on an EC2-Classic instance and deployed in the public subnet. As part of security monitoring, the networking team needs to get the list of the requester IP addresses going to your EC2 instances. Which of the following would help in fulfilling this requirement?

Utilize CloudWatch logs to check the requesting IP addresses.

Explanation:-This option is incorrect because CloudWatch logs will not give you the IP addresses coming into your EC2 instances.

Enable VPC Flow Logs for your VPC.

Explanation:-This option is incorrect because the VPC Flow Logs cannot be enabled for the network interfaces that are in the EC2-Classic platform.

Migrate your application to an EC2-VPC instance then enable VPC Flow Logs for your VPC.

Explanation:-This option is the correct answer. Take note that you cannot enable flow logs for network interfaces that are in the EC2-Classic platform. This includes EC2-Classic instances that have been linked to a VPC through ClassicLink.

VPC Flow logs enable you to capture information about the IP traffic going to and from the network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. You can also use flow logs as a security tool to monitor the traffic that

Enable AWS CloudTrail service to log all requests on your AWS resources.

Explanation:-This option is the incorrect because this is an API monitoring service that provides event histories of your AWS account activity.

Q38) A tech company is moving their on-premises database to AWS but still undecided if they want to use RDS or just an EC2 instance. As their Systems Administrator, you are responsible to know the database-related activities that will be performed by AWS, which would eventually lessen the administrative activities of their IT Operations team.
Which of the following is carried out by AWS for database hosted in the AWS RDS service? (Choose 2)

Automatically deploy RDS Read Replicas when the database utilization is high.

Explanation:-This option is incorrect because RDS does not automatically create Read Replicas nor set up a Multi-AZ deployments configuration.

Automatically configure the RDS instance to use Multi-AZ deployments configuration.

Explanation:-This option is incorrect because RDS does not automatically create Read Replicas nor set up a Multi-AZ deployments configuration.

Critical security patches installation.

Explanation:-Periodically, Amazon RDS performs maintenance on Amazon RDS resources. Maintenance most often involves updates to the DB instance's underlying operating system (OS) or database engine version. Updates to the operating system most often occur for security issues and should be done as soon as possible.

You can restore a DB instance to a specific point in time, creating a new DB instance. RDS uploads transaction logs for DB instances to Amazon S3 every 5 minutes.

Query Optimization.

Explanation:-This option is incorrect because the customer is responsible for applying query optimizations for the database to improve its performance.

Create and maintain backups with a long term retention of 1 year.

Explanation:-This option is incorrect because the maximum retention period possible for RDS databases is only 35 days and not 1 year.

Create and maintain backups with a point in time recovery of 5 minutes.

Explanation:-Periodically, Amazon RDS performs maintenance on Amazon RDS resources. Maintenance most often involves updates to the DB instance's underlying operating system (OS) or database engine version. Updates to the operating system most often occur for security issues and should be done as soon as possible.

You can restore a DB instance to a specific point in time, creating a new DB instance. RDS uploads transaction logs for DB instances to Amazon S3 every 5 minutes.

Q39) A distributed transaction processing system is deployed in AWS which consists of an Auto Scaling group of Spot EC2

instances and an SQS queue for messaging. You have to ensure that there is a separate queue for the messages which are not processed successfully.
Which of the following options would you configure for this task?

- Standard Queues

Explanation:-This option is incorrect.

- FIFO Queues

Explanation:-This option is incorrect.

- Delay Queues

Explanation:-This option is incorrect.

- ✅ Dead-Letter Queues

Explanation:-Amazon SQS supports dead-letter queues, which other queues (source queues) can target for messages that can't be processed (consumed) successfully. Dead-letter queues are useful for debugging your application or messaging system because they let you isolate problematic messages to determine why their processing doesn't succeed.
When you designate a queue to be a source queue, a dead-letter queue is not created automatically. You must first create a normal standard or FIFO queue before desig

---

Q40) You are working as a Junior SysOps Administrator for a multinational insurance firm. To ensure the security of sensitive financial data, an IT auditor checked the OS patching process of your RDS instances for any vulnerability that can put the entire firm at risk.
Which AWS service can you use to report in this scenario?

- Amazon Inspector

Explanation:-This option is incorrect.

- ✅ Amazon RDS Console

Explanation:-In this scenario, you can simply check the Amazon RDS console to view if your RDS instance needs OS patching. Periodically, Amazon RDS performs maintenance on Amazon RDS resources. Maintenance most often involves updates to the DB instance's underlying operating system (OS) or database engine version. Updates to the operating system most often occur for security issues and should be done as soon as possible.
Maintenance items require that Amazon RDS take your DB instance offline for a short

- AWS Artifact

Explanation:-This option is incorrect.

- AWS Trusted Advisor

Explanation:-This option is incorrect.

Q41)

You are required to track the usage of your cloud resources against the AWS service limit.

For easier tracking, your team should be notified in your existing Slack channel whenever you are approaching a given limit which will allow you to proactively request a service limit increase or shut down resources before you exceed the limit.

Which of the following is the most suitable solution that you should implement to meet this requirement?

- ✅ Set up AWS Limit Monitor by using AWS Lambda, AWS Trusted Advisor, and CloudWatch Events rules to track and monitor your AWS service limits which would be sent to your Slack Channel.

Explanation:-To help provide highly-available, reliable, and robust services to all customers, as well as minimize billing risk for new customers, Amazon Web Services (AWS) maintains service limits for each account. Nearly every AWS service is regulated in terms of how many resources you can launch within a specific AWS Region at a given time. However, there are times when even the most experienced AWS customers can unexpectedly hit service limits.
To help customers more actively track their AWS resourc

- Use CloudWatch and SNS then enable Enhanced Monitoring which will automatically send messages to your Slack channel when you are about to hit your AWS service limit.

Explanation:-This option is incorrect because the Enhanced Monitoring feature in CloudWatch simply increases the frequency of your metric data from the standard 5-minute periods to 1-minute.

- Use a combination of AWS Inspector to track the service limits and SNS to send messages to your Slack channel.

Explanation:-This option is incorrect because Amazon Inspector is just an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. This service does not track the Service Limits of your AWS account.

- Set up a scheduled Lambda function that queries the AWS Trusted Advisor - Service Limits to track the usage and limits of your AWS account. Integrate the function with SES to automatically send an email to your Slack channel

Explanation:-This option is incorrect. Although it is correct to set up a scheduled Lambda function that queries the AWS Trusted Advisor - Service Limits, the use of Amazon Simple Email Service (SES) to send an email to your Slack channel is wrong. You should use another Lambda function or SNS, instead of SES, to integrate with Slack.

Q42) You are hosting a video streaming website in AWS CloudFront. There are times that your website receives malicious attacks such as SQL injection and DDoS attacks from different unknown origins. Customers are affected because they have a hard time accessing your website during these outages.
Which of the following services mitigates these kinds of attacks?

- AWS Artifact

Explanation:-This option is incorrect.

- ✅ AWS WAF & Shield

Explanation:-You use AWS WAF to control how Amazon CloudFront or an Application Load Balancer responds to web requests. You start by creating conditions, rules, and web access control lists. You define your conditions, combine your conditions into rules, and combine the rules into a web ACL.
AWS Shield provides protection against DDoS attacks. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services. For added protection against D

- AWS Guard Duty

Explanation:-This option is incorrect.

AWS Inspector

Explanation:-This option is incorrect.

Q43) An online banking system will be deployed to AWS which will be utilizing an Auto Scaling group of EC2 instances, an Application Load Balancer, and an RDS instance. To secure the personal data of the clients, you need to enable encryption for the DB instance.
Which of the following are invalid limitations of an Amazon RDS encrypted DB instance? (Choose 2)

Encrypted Read Replicas must be encrypted with the same key as the source DB instance

Explanation:-This option is incorrect.

✓ You can restore an unencrypted backup or snapshot to an encrypted DB instance.

Explanation:-The following limitations exist for Amazon RDS encrypted DB instance:
• You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created. However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted sn

You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created.

Explanation:-This option is incorrect.

To copy an encrypted RDS snapshot from one region to another, you must specify the KMS key identifier of the destination region.

Explanation:-This option is incorrect.

DB instances that are encrypted can't be modified to disable encryption.

Explanation:-This option is incorrect.

✓ You can have an encrypted Read Replica of an unencrypted DB instance or an unencrypted Read Replica of an encrypted DB instance.

Explanation:-The following limitations exist for Amazon RDS encrypted DB instance:
• You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created. However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted sn

---

Q44) You have a third-party vendor that needs access to an AWS resource in your company's account to complete their integration project. After creating an AWS user account for the vendor, you want to restrict their access to specific AWS resources that they only need using an IAM policy and only for 2 weeks.
Which of the following options would be an ideal policy to use?

A Bucket ACL

Explanation:-This option is invalid because they are specifically meant for access to S3 buckets.

A Bucket Policy

Explanation:-This option is invalid because they are specifically meant for access to S3 buckets.

✓ An Inline Policy

Explanation:-This is the correct answer. Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that it's applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Manag

An AWS Managed Policy

Explanation:-This option is invalid because AWS Managed Policies are recommended to use for a group of users. For individual users, inline policies are better.

Q45) A newly hired SysOps Engineer is given the task to manage S3 bucket policies in your AWS accounts. She will first need to understand how policies are created and how to apply them to the buckets.
In this case, what does the following S3 policy do?

```
1. {
2. "Version":"2012-10-17",
3. "Statement":[
4. {
5. "Sid":"AddCannedAcl",
6. "Effect":"Allow",
7. "Principal": {"AWS": ["arn:aws:iam::111122223333:root","arn:aws:iam::444455556666:root"]},
8. "Action":["s3:PutObject","s3:PutObjectAcl"],
9. "Resource":["arn:aws:s3:::tutorialsdojo/*"],
10. "Condition":{"StringEquals":{"s3:x-amz-acl":["public-read"]}}
11. }
12. ]
13. }
```

It is granting cross-account permissions to upload objects while ensuring the bucket owner has full control.

Explanation:-This option is incorrect answers because fulfilling these permissions require different S3 bucket policies. Examples of policies that provide the aforementioned permissions can be found in the reference link.

It is granting permissions to an Amazon CloudFront Origin Identity.

Explanation:-This option is incorrect answers because fulfilling these permissions require different S3 bucket policies. Examples of policies that provide the aforementioned permissions can be found in the reference link.

✓ It is granting permissions to multiple accounts with added conditions.

Explanation:-This is the correct answer because the following example policy grants the s3:PutObject and s3:PutObjectAcl permissions to multiple AWS accounts and requires that any request for these operations include the public-read canned ACL.

It is granting read-only permissions to anonymous users.

Explanation:-This option is incorrect answers because fulfilling these permissions require different S3 bucket policies. Examples of policies that provide the aforementioned permissions can be found in the reference link.

Q46) You have a NodeJS application running on an On-Demand EC2 instance which requires temporary credentials for authentication, and permissions to authorize the application to perform actions in AWS. To properly set up the application, you are required to pass a role to EC2 to use with the instance that provides those credentials.
Which of the following IAM actions should you define in your IAM policy to enable the user to pass a role to an AWS service?

✅ PassRole

Explanation:-To configure many AWS services, you must pass an IAM role to the service. This allows the service to later assume the role and perform actions on your behalf. You only have to pass the role to the service once during setup, and not every time that the service assumes the role.

For example, assume that you have an application running on an Amazon EC2 instance. That application requires temporary credentials for authentication, and permissions to authorize the application to perform actions i

⚪ AttachRolePolicy

Explanation:-This option is incorrect because the AttachRolePolicy just grants permission to attach a managed policy to the specified IAM role. This does not enable the user to pass a role.

⚪ PassedToService

Explanation:-This option is incorrect because PassedToService is just a condition key, and not an IAM action per se, that filters access by the AWS service to which this role is passed.

⚪ AddRoleToInstanceProfile

Explanation:-This option is incorrect because the AddRoleToInstanceProfile simply grants permission to add an IAM role to the specified instance profile, but not pass a role.

Q47) A top investment bank has a set of Customer Master Keys defined in AWS Key Management Service to secure their financial data. As the Systems Administrator, you need to review who has access to which keys to prevent any security breach. In addition, you need to make the required changes based on the policy documents defined by the company.
Where could you make changes to who can access the keys in the KMS service?

✅ Key Policies

Explanation:-This is the correct answer. Key policies are the primary way to control access to customer master keys (CMKs) in AWS KMS. Although they are not the only way to control access, you cannot control access without them.

⚪ Object Access Control Lists

Explanation:-This option is invalid because these are referent to access policies for S3.

⚪ Bucket Policies

Explanation:-This option is invalid because these are referent to access policies for S3.

⚪ KMS Policies

Explanation:-This option is invalid because there are no KMS policies.

Q48) A leading telecommunications company has decided to host their e-commerce website in an Auto Scaling group of EC2 instances and a RDS database instance for their mobile phone plans. To secure the online transactions, you were instructed to configure the database to encrypt the data in transit.
Which of the following should you do to meet the requirements?

✅ Based on its respective DB engine, configure the database to use SSL and use the certificates which are readily available from AWS.

Explanation:-You can use SSL from your application to encrypt a connection to a DB instance running MySQL, MariaDB, SQL Server, Oracle, or PostgreSQL. Each DB engine has its own process for implementing SSL.

A root certificate that works for all regions can be downloaded from the AWS website. It is the trusted root entity and should work in most cases but might fail if your application doesn't accept certificate chains. If your application doesn't accept certificate chains, download the AWS Region–speci

⚪ Do nothing. By default, RDS already provides data encryption for data at rest.

Explanation:-This option is incorrect because RDS does not provide the SSL connection by default.

⚪ Use the CloudHSM service to encrypt the incoming and outgoing traffic to RDS.

Explanation:-This option is incorrect because CloudHSM is just a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys. It does not provide you a way to configure your RDS database instance to use SSL.

⚪ Use a VPC endpoint, which is powered by AWS PrivateLink, that enables you to connect to the RDS database instance.

Explanation:-This option is incorrect because a VPC endpoint is primarily used to privately connect your VPC to other AWS services and endpoint services. It does not provide SSL connection to your RDS database.

Q49) A supermarket chain is using an S3 bucket to store the media files of its various products which are used on its e-commerce website. The users of the S3 bucket should only be able to read and write objects but not delete any objects.
Which of the following should you set up to meet this requirement?

⚪ Enable CRR for the S3 bucket.

Explanation:-This option is incorrect because CRR is mainly used for Cross region replication for the bucket objects.

⚪ Enable MFA Delete on the bucket.

Explanation:-This is incorrect because enabling MFA Delete is primarily used to prevent accidental deletion of objects from the bucket. Even though you have this feature enabled, the users can still delete objects as long as they have a valid MFA device and had been authenticated properly.

✅ Attach an S3 bucket policy.

Explanation:-By default, all Amazon S3 resources such as buckets, objects, and related subresources (for example, lifecycle configuration and website configuration) are private which means that only the resource owner, an AWS account that created it, can access the resource. The resource owner can optionally grant access permissions to others by writing an access policy.

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to

⚪ Enable Versioning on the S3 bucket.

Explanation:-This option is incorrect because enabling the versioning option in an S3 bucket does not prevent the users from deleting objects.

Q50) You are working as the Lead Systems Administrator for a digital design company which is planning to launch a set of AWS resources that consists of EC2 Instances and an RDS Instance. The CTO asked you to prepare the technical documents which states the scope and responsibilities of your team and of AWS when it comes to the maintenance of the cloud infrastructure.
Which of the following is not the responsibility of AWS? (Choose 2)

⚪ Inventory management for the underlying infrastructure devices.

Explanation:-This option is incorrect because patch and inventory management of the underlying physical servers is the responsibility of AWS.

✅ Inventory management for the underlying databases.

Explanation:-Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as we

Patch management of the underlying physical servers.

Explanation:-This option is incorrect because patch and inventory management of the underlying physical servers is the responsibility of AWS.

Patch management of the underlying guest OS.

Explanation:-Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as we

---

Q51) You are working as SysOps Administrator for a financial services company which has multiple EC2 instances deployed in a private subnet that needs to use the Amazon KMS service. Due to the company's strict security requirements, the traffic should not pass through the public Internet even if the financial data have already been encrypted by KMS.
Which of the following would help you meet this requirement?

VPC endpoint

Explanation:-You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint, communication between your VPC and AWS KMS is conducted entirely within the AWS network. AWS KMS supports Amazon Virtual Private Cloud (Amazon VPC) interface endpoints that are powered by AWS PrivateLink. Each VPC endpoint is represented by one or more Elastic Network Interfaces (ENIs) with private IP addresses in your VPC subnets.
The VPC interfac

VPN connection

Explanation:-This option is incorrect because a VPN connection passes through the public Internet. You have to use a VPC endpoint to privately connect to various cloud services provided by AWS.

NAT gateway

Explanation:-This option is incorrect because both NAT Instance and NAT gateway are primarily used to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet or other AWS services, but prevent the instances from receiving inbound traffic initiated by someone on the Internet.

NAT Instance

Explanation:-This option is incorrect because both NAT Instance and NAT gateway are primarily used to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet or other AWS services, but prevent the instances from receiving inbound traffic initiated by someone on the Internet.

Q52) A mobile game development company has recently launched an app that gamifies personal finance which allows the users to earn points for every dollar they save or earn. They are using Kinesis Data Streams to continuously collect data about player-game interactions and feed the data into their mobile gaming platform. Due to the sensitive financial data that the application collects, you were instructed to configure your AWS resources to be secured at rest.
Which of the following should you do to meet the requirement?

Data encryption is not supported in Amazon Kinesis Data Streams hence, you should develop a custom encryption service to secure your data at rest.

Explanation:-This option is incorrect because Amazon Kinesis Data Streams does support data encryption.

Configure Amazon Kinesis Data Streams to use client-side encryption.

Explanation:-This option is incorrect because the scenario requires you to secure your data at rest and not in transit, which means that you need to enable server-side encryption.

Configure Amazon Kinesis Data Streams to use SSL.

Explanation:-This option is incorrect because SSL secures your data in transit and not at rest.

Configure Amazon Kinesis Data Streams to use server-side encryption.

Explanation:-Server-side encryption is a feature in Amazon Kinesis Data Streams that automatically encrypts data before it's at rest by using an AWS KMS customer master key (CMK) you specify. Data is encrypted before it's written to the Kinesis stream storage layer, and decrypted after it's retrieved from storage. As a result, your data is encrypted at rest within the Kinesis Data Streams service. This allows you to meet strict regulatory requirements and enhance the security of your data.

Q53) You are working as a Senior Systems Engineer for a technology company where you are instructed to ensure that all objects in their S3 bucket are encrypted at rest. In addition, you also need to configure the proper permissions for the bucket.
Which of the following is required to properly implement this requirement?

Configure the S3 bucket to deny all requests if the x-amz-meta-x-amz-key header is not included.

Explanation:-This option is incorrect because the x-amz-meta-x-amz-key is primarily used for client-side encryption to protect the data in transit to S3.

Configure the S3 bucket to deny all requests if the x-amz-server-side-encryption-context header is not included.

Explanation:-This option is incorrect because the x-amz-server-side-encryption-context header is basically just an optional encryption context and you still need to use the x-amz-server-side-encryption header.

Configure the S3 bucket to deny all requests if the x-amz-server-side-encryption-aws-kms-key-id header is not included

Explanation:-This option is incorrect because the x-amz-server-side-encryption-aws-kms-key-id header is a condition key which you can use to require a specific KMS key for object encryption. Although this is a valid answer, remember that this header is only optional and you still need to use the x-amz-server-side-encryption header.

Configure the S3 bucket to deny all requests if the x-amz-server-side-encryption header is not included.

Explanation:-Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Q54)

An online stocks trading platform is hosted on an Amazon ECS Cluster using a MySQL RDS instance.

The IT Security department of the company requires that all data stored in your cloud architecture be encrypted at rest which means that you have to encrypt the data residing in your RDS instance.

Which of the following options is not true regarding Amazon RDS Encrypted DB Instance? (Choose 2)

✅ DB instances that are encrypted can be modified to disable encryption.
Explanation:-The following limitations exist for Amazon RDS encrypted DB instance:
• You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created.
• However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encr
⚪ Encrypted Read Replicas must be encrypted with the same key as the source DB instance.
Explanation:-This option is incorrect.
⚪ You can't have an encrypted Read Replica of an unencrypted DB instance or an unencrypted Read Replica of an encrypted DB instance.
Explanation:-This option is incorrect.
✅ You can restore an unencrypted backup or snapshot to an encrypted DB instance.
Explanation:-The following limitations exist for Amazon RDS encrypted DB instance:
• You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created.
• However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encr
⚪ To copy an encrypted snapshot from one region to another, you must specify the KMS key identifier of the destination region.
Explanation:-This option is incorrect.
⚪ You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created.

Q55) A legacy web application in your VPC is hosted on a set of EC2 instances with a Classic Load balancer in front to evenly distribute the traffic across two Availability Zones: us-west-2a and us-west-2b. The EC2 instances in the us-west-2a Availability Zone are experiencing high latency and are slow to respond to requests. As a result, the surge queue for the load balancer node in us-west-2a Availability Zone exceeds its limit.
Which of the following metrics can provide you with the total number of requests that were rejected when the surge queue is full?

✅ SpilloverCount
Explanation:-The SpilloverCount provides the total number of requests that were rejected because the surge queue is full.
Suppose that your load balancer has us-west-2a and us-west-2b enabled, and that instances in us-west-2a are experiencing high latency and are slow to respond to requests. As a result, the surge queue for the load balancer node in us-west-2a fills, resulting in spillover. If us-west-2b continues to respond normally, the sum for the load balancer will be the same as the sum for us-west
⚪ BackendConnectionErrors
Explanation:-This option is incorrect because BackendConnectionErrors is the number of connections that were not successfully established between the load balancer and the registered instances.
⚪ HealthyHostCount
Explanation:-This option is incorrect because HealthyHostCount is the number of healthy instances registered with your load balancer. A newly registered instance is considered healthy after it passes the first health check.
⚪ SurgeQueueLength
Explanation:-This option is incorrect because the SurgeQueueLength metric provides the total number of requests (HTTP listener) or connections (TCP listener) that are pending routing to a healthy instance.

Q56) An online gaming site is hosted on a single EC2 Instance with a DynamoDB database. They are planning to release a new game and hence, it is necessary to ensure the availability of their website to cater the surge of new players using their platform.
Which of the following is the easiest way to achieve this requirement?

⚪ Terminate the EC2 instance and then re-launch it using a new OpsWorks stack.
Explanation:-This option is incorrect.
⚪ Terminate the EC2 instance and launch it again using a new Elastic Beanstalk environment.
Explanation:-This option is incorrect.
✅ Create an Auto Scaling Group out of the running EC2 Instance.
Explanation:-Amazon EC2 Auto Scaling provides you with an option to create a launch configuration using the attributes from a running EC2 instance. You can create an Auto Scaling group directly from an EC2 instance. When you use this feature, Amazon EC2 Auto Scaling automatically creates a launch configuration for you as well.
If the specified instance has properties that are not currently supported by launch configurations, the instances launched by the Auto Scaling group might not be identical to the
⚪ Generate a custom AMI out of the running EC2 instance then terminate the instance once the process is complete. Create a new launch configuration using the custom AMI and then launch the Auto Scaling Group.
Explanation:-This option is incorrect.

Q57)

An online food delivery website is hosted in an Amazon ECS Cluster and is using an RDS database instance.

The company has recently deployed the new version of their delivery website which uses DynamoDB instead of RDS. Your manager instructed you to disable the backups of your RDS instance as these will no longer be used.

You were able to successfully set the retention period to 1 with no issues but you encountered an error when you tried to set this at 0.

Which of the following could be the possible reason for this issue?

✅ The RDS instance has Read Replicas.
Explanation:-There are several reasons why you may need to set the backup retention period to 0. For example, you can disable automatic backups immediately by setting the retention period to 0. If you set the value to 0 and receive a message saying that the retention period must be between 1 and 35, check to make sure you haven't setup a read replica for the instance. Read replicas require backups for managing read replica logs, thus, you can't set the retention period of 0.
⚪ You do not have the required IAM access to configure your RDS instance.

Explanation:-This option is incorrect because although it can be a valid answer, you were able to set it to 1 without issues. This means that you already have the required IAM policy.

- The RDS instance is using a Multi-AZ deployments configuration.

Explanation:-This option is incorrect because a Multi-AZ deployments configuration should have no effect on setting the backup retention period.

- The minimum retention period that you can set is 1.

Explanation:-This option is incorrect because the minimum retention period that you can set is 0 and not 1.

Q58) A web application is hosted on 4 On-Demand EC2 instances which are deployed evenly across two Availability Zones behind a Classic Load Balancer. Based on your CloudWatch monitoring, one of the EC2 instances is running at approximately 95% CPU utilization while the other three instances only have 10% CPU utilization.
Which of the following is the most suitable fix for this issue?

- Replace your Classic Load Balancer with an Application Load Balancer.

Explanation:-This option is incorrect because although an Application Load Balancer has more features than Classic Load Balancer, this solution entails an architecture change on your part and may take a lot of time. It is still better to disable sticky sessions that will immediately fix the issue.

- Disable connection draining in the Classic Load Balancer.

Explanation:-This option is incorrect because the connection draining feature simply enables the load balancer to complete in-flight requests made to instances that are de-registering or unhealthy.

- ✅ Disable the sticky sessions feature of the Classic Load Balancer.

Explanation:-By default, a Classic Load Balancer routes each request independently to the registered instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance. However, there are some cases where majority of the incoming traffic is always routed on a specific EC2 instance.

- Disable Cross-zone load balancing in the Classic Load Balancer.

Explanation:-This option is incorrect because a cross-zone load balancing just sets each load balancer node of your Classic Load Balancer to distribute requests evenly across the registered instances in all enabled Availability Zones. The issue is the high CPU Utilization of one of the EC2 instances because it is bound to a user's session, which can be solved by disabling the sticky sessions.

Q59)

You have been instructed by your manager to set up the architecture of a web application in AWS. It should be deployed on an Auto Scaling group of EC2 Instances with an Elastic Load Balancer in front to evenly distribute the incoming traffic.

You were also instructed to route certain requests to specific target groups based on the URL paths.

The EC2 instances should also be able to withstand CPU bursts for long periods of time.

Which of the following options should you do to ensure that you are deploying the application to AWS in a cost-effective manner? (Choose 2)

- Use a Classic Load Balancer.

Explanation:-This option is incorrect as both Classic Load Balancer and Network Load Balancer do not support path-based routing.

- Deploy a burstable general-purpose instance type such as T2 instances that are cost-effective.

Explanation:-This option is incorrect because although T2 is cost-effective, it cannot sustain high CPU performance. You should have used T2 Unlimited instead.

- Use a Network Load Balancer.

Explanation:-This option is incorrect as both Classic Load Balancer and Network Load Balancer do not support path-based routing.

- ✅ Use an Application Load Balancer.

Explanation:-Burstable performance instances, which include T3 and T2 instances, are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload. Burstable performance instances are well suited for a wide range of general-purpose applications. Examples include microservices, low-latency interactive applications, small and medium databases, virtual desktops, development, build, and stage environments, code repositories, and product prototy

- ✅ Deploy a burstable general-purpose instance type such as T2 Unlimited or T3 instances in Unlimited mode.

Explanation:-Burstable performance instances, which include T3 and T2 instances, are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload. Burstable performance instances are well suited for a wide range of general-purpose applications. Examples include microservices, low-latency interactive applications, small and medium databases, virtual desktops, development, build, and stage environments, code repositories, and product prototy

- Enable Enhanced Networking in the EC2 instances.

Explanation:-This option is incorrect.

Q60) A clothing company is hosting an e-commerce website that receives a lot of traffic during winter because of the massive sale on their jackets, sweaters, and beanies. During this peak season, you want your AWS resources to automatically scale to an optimal amount across all the Availability Zones to support the demands of your customers. The resources that you are currently running in the cloud are EC2 instances with an ELB, Aurora DB clusters, and a DynamoDB database.
Which of these choices cannot be scaled using AWS Auto Scaling?

- EC2 instances with ELB

Explanation:-This option is incorrect.

- Aurora DB clusters

Explanation:-This option is incorrect.

- DynamoDB tables

Explanation:-This option is incorrect.

- ✅ None of these

Explanation:-This option is the correct answer. AWS Auto Scaling automatically scales the following resources that support your application: Amazon EC2 Auto Scaling groups, Aurora DB clusters, DynamoDB global secondary indexes, DynamoDB tables, ECS services, and Spot Fleet requests.
You should use EC2 Auto Scaling if you only need to scale Amazon EC2 Auto Scaling groups, or if you are only interested in maintaining the health of your EC2 fleet.

Q61) A company has multiple AWS accounts which are consolidated with AWS Organizations. You are instructed to ensure that the tags are consistently applied when your resources are created in AWS across all accounts.
Which of the following options should you do to satisfy this requirement? (Choose 2)

- Use AWS generated tags by activating it in the Billing and Cost Management console of the member account.

Explanation:-This option is incorrect because although you can use the AWS generated tags feature in this scenario, you have to activate it using the master account and not on the member account.

- Use AWS Config to add the corresponding tags to your resources after they are created.

Explanation:-This option is incorrect because although you can use AWS Config to determine if your resources have tags or not, it does not have the capability to add the corresponding tags to your resources. However, you can use AWS Service Catalog in conjunction with AWS Config to satisfy the requirement.

- Use AWS Systems Manager Automation to automatically add tags to your provisioned resources.

Explanation:-This option is incorrect because you cannot automatically add tags to your provisioned resources using AWS Systems Manager Automation.

- ✅ Use AWS Service Catalog to tag the provisioned resources with corresponding unique identifiers for portfolio, product, and users.

Explanation:-AWS offers a variety of tools to help you implement proactive tag governance practices by ensuring that tags are consistently applied when resources are created.
AWS CloudFormation provides a common language for provisioning all the infrastructure resources in your cloud environment. CloudFormation templates are simple text files that create AWS resources in an automated and secure manner. When you create AWS resources using AWS CloudFormation templates, you can use the CloudFormation Resou

- ✅ Use the CloudFormation Resource Tags property to apply tags to certain resource types upon creation.

Explanation:-AWS offers a variety of tools to help you implement proactive tag governance practices by ensuring that tags are consistently applied when resources are created.
AWS CloudFormation provides a common language for provisioning all the infrastructure resources in your cloud environment. CloudFormation templates are simple text files that create AWS resources in an automated and secure manner. When you create AWS resources using AWS CloudFormation templates, you can use the CloudFormation Resou

---

Q62) You want to control the costs of your usage in AWS Cloud. Since AWS offers flexible services and pricing options that allow you to pay only for the services you need yet still meet your performance and capacity requirements, knowing cost optimization best practices will benefit you well.
Which of the following practices will help you optimize costs? (Choose all that applies)

- ✅ Measure and monitor resource charges using cost management tools.

Explanation:-This option will help you optimize costs since provisioning the right size for EC2 instances allows you to maximize usage while saving costs. Automating elasticity of resources will allow you to meet demands in a more fluid manner by adding and deleting instances as necessary. Selecting the correct storage tier for your EBS will also make the most out of it. Finally, by measuring and monitoring resource charges, you can keep track of billing and learn how to manage it.

- Use Reserved EC2 Instances even though you won't be utilizing them all the time because of the large discounts offered.

Explanation:-This option is incorrect because, depending on your usage, you might find it cheaper to use other types of instances instead of reserved instances or a hybrid of these types. Reserved Instances also require you to commit to 1-year or 3-year terms, which has different characteristics.

- ✅ Select the correct storage tier for your EBS without compromising performance.

Explanation:-This option will help you optimize costs since provisioning the right size for EC2 instances allows you to maximize usage while saving costs. Automating elasticity of resources will allow you to meet demands in a more fluid manner by adding and deleting instances as necessary. Selecting the correct storage tier for your EBS will also make the most out of it. Finally, by measuring and monitoring resource charges, you can keep track of billing and learn how to manage it.

- ✅ Automate elasticity of resources by using Auto Scaling Groups to meet dynamic needs.

Explanation:-This option will help you optimize costs since provisioning the right size for EC2 instances allows you to maximize usage while saving costs. Automating elasticity of resources will allow you to meet demands in a more fluid manner by adding and deleting instances as necessary. Selecting the correct storage tier for your EBS will also make the most out of it. Finally, by measuring and monitoring resource charges, you can keep track of billing and learn how to manage it.

- Use EC2 Spot instances all the time for cheaper pricing options.

Explanation:-This option is incorrect because spot instances are only available as long as your bidding price is not outbid by another bidder. Although spot instances are cheap, they are also volatile as the instances can be terminated by AWS. This means that you may suddenly lose instances during critical business operation times.

- ✅ Provision the right sizing for EC2 instances.

Explanation:-This option will help you optimize costs since provisioning the right size for EC2 instances allows you to maximize usage while saving costs. Automating elasticity of resources will allow you to meet demands in a more fluid manner by adding and deleting instances as necessary. Selecting the correct storage tier for your EBS will also make the most out of it. Finally, by measuring and monitoring resource charges, you can keep track of billing and learn how to manage it.

Q63) An innovative startup company has hired you to be their Systems Administrator to handle their various applications hosted in AWS, such as peer-to-peer ride-sharing, bicycle-sharing, food delivery, and many others. You need to ensure that all of their custom baked AMI's are kept up-to-date with the latest patches to avoid any security vulnerability.
Which of the following can help you automate this requirement?

- AWS OpsWorks Chef Automate

Explanation:-This option is incorrect because Chef Automate is a suite of automation tools from Chef mainly used for configuration management, compliance and security, and continuous deployment.

- EC2 Dashboard

Explanation:-This option is incorrect because the EC2 Dashboard will just give information and services that you can use with EC2.

- ✅ AWS Systems Manager Automate

Explanation:-This option is the correct answer. Systems Manager Automation is an AWS-hosted service that simplifies common instance and system maintenance and deployment tasks. Automation offers one-click automations for simplifying complex tasks such as creating golden Amazon Machines Images (AMIs), and recovering unreachable EC2 instances.

- AWS Trusted Advisor

Explanation:-This option is incorrect because Trusted Advisor is just an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment.

Q64) An application is hosted in an Auto Scaling group of t2.small EC2 instances in your VPC. You noticed that when the workload goes up, the EC2 instances experience networking issues that affect the entire application.
Which of the following can you do to resolve the issue?

- Attach a Provisioned IOPS EBS volume on each EC2 instances.

Explanation:-This option is incorrect because changing the EBS volume will not improve the network performance. You have to upgrade your EC2 instances to a higher instance type.

- Attach an Optimized EBS volume on each EC2 instances.

Explanation:-This option is incorrect because changing the EBS volume will not improve the network performance. You have to upgrade your EC2 instances to a higher instance type.

- Use a secondary ENI on all EC2 instances.

Explanation:-This option is incorrect because adding an ENI will not resolve the problem as this is only an interface.

- ✅ Upgrade the EC2 instance to a larger instance type.

Explanation:-Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more instance sizes, allowing you to scale your resources to the requirements of your target workload.
T2 instances are Burstable Performance Instances that provide a baseline le

---

Q65) A digital advertising company has a large MySQL RDS database which is being heavily used by their suite of data analytics applications. Lately, there are a lot of performance issues happening on your applications in production and after further investigation, it was discovered that the database could not handle the high volume of incoming read requests.
Which of the following options can be done to alleviate the performance issue of the database? (Choose 2)

- Put the EC2 instances behind a load balancer to increase overall performance.

Explanation:-This option is incorrect because the RDS instance is separate from the EC2 instance. Increasing IOPS on EC2 or adding an ELB in front of it will not affect the database throughput.

- Enable Multi-AZ for the database.

Explanation:-This option is incorrect because Multi-AZ is used for high availability of databases.

- Provision more IOPS on the EBS volume of the Application to increase the I/O throughput.

Explanation:-This option is incorrect because the RDS instance is separate from the EC2 instance. Increasing IOPS on EC2 or adding an ELB in front of it will not affect the database throughput.

- ✅ Add a Read Replica for the database.

Explanation:-This option is correct. This is called horizontal scaling. In addition to scaling your master database vertically, you can also improve the performance of a read-heavy database by using read replicas to horizontally scale your database. RDS MySQL, PostgreSQL, and MariaDB can have up to 5 read replicas, and Amazon Aurora can have up to 15 Read Replicas.

- Add a CloudFront distribution in front of the load balancer.

Explanation:-This option is incorrect because CloudFront is a Content Delivery Service (CDN) service and is normally used for web distributions.

- ✅ Upgrade the Instance type for the underlying database server.

Explanation:-This option is correct. This is called vertical scaling. To handle a higher load in your database, you can vertically scale up your master database with a simple push of a button. There are currently over 18 instance sizes that you can choose from when resizing your RDS MySQL, PostgreSQL, MariaDB, Oracle, or Microsoft SQL Server instance. For Amazon Aurora, you have 5 memory-optimized instance sizes to choose from. The wide selection of instance types allows you to choose the best resource and c

---