Answer Sheet

Q1) A company plans to deploy a fleet of On-Demand EC2 instances which are expected to have fairly constant workloads that translates to a CPU utilization of around 40% with brief intervals of peak loads.
Which of the following would be the most cost-effective instance types that can be used? (Choose 2)

✅ T3 Instance type
Explanation:-In this scenario, you can use T2 and T3 instances to prove a baseline level of CPU performance for your fleet of EC2 instances. It can also provides the ability to burst CPU usage to handle the ocassional peak loads.
T2 instances are Burstable Performance Instances that provide a baseline level of CPU performance with the ability to burst above the baseline. T2 Unlimited instances can sustain high CPU performance for as long as a workload needs it. For most general-purpose workloads, T2 Unl
⚪ H1 Instance type
⚪ M4 Instance type
⚪ C4 Instance type
⚪ I3 Instance type
✅ T2 Instance type
Explanation:-In this scenario, you can use T2 and T3 instances to prove a baseline level of CPU performance for your fleet of EC2 instances. It can also provides the ability to burst CPU usage to handle the ocassional peak loads.
T2 instances are Burstable Performance Instances that provide a baseline level of CPU performance with the ability to burst above the baseline. T2 Unlimited instances can sustain high CPU performance for as long as a workload needs it. For most general-purpose workloads, T2 Unl

---

Q2) You are working as a SysOps Administrator in a leading tech consultancy firm which has an AWS Virtual Private Cloud (VPC) with one public subnet. The firm has a new blockchain application which you deployed to an m3.large EC2 instance. After a month, your manager instructed you to ensure that the application can support IPv6 address.
Which of the following steps would you follow to satisfy the requirement?

⚪ 1. Associate an IPv6 CIDR Block with Your VPC and Subnets2. Update Your Route Tables3. Update Your Security Group Rules4. Assign IPv6 Addresses to Your Instances5. Configure the instance to use DHCPv6
Explanation:-The options sequence is incorrect.
⚪ 1. Associate an IPv6 Gateway with the VPC and Subnets2. Update the Route Tables3. Update the Security Group Rules4. Assign IPv6 Addresses to the EC2 instance5. Configure the instance to use DHCPv6
Explanation:-The options sequence is incorrect.
✅ 1. Associate an IPv6 CIDR Block with the VPC and Subnets2. Update the Route Tables3. Update the Security Group Rules4. Change the Instance Type to m4.large5. Assign IPv6 Addresses to the EC2 Instance
Explanation:-Take note that the EC2 instance is an m3.large instance type, which does not support IPv6. You must resize the instance to a supported instance type, for example, m4.large. Since only Option 3 has this step out of all the options, then this is the correct answer. Remember that configuring an IPv6 is just an optional step.
If you have an existing VPC that supports IPv4 only, and resources in your subnet that are configured to use IPv4 only, you can enable IPv6 support for your VPC and resour
⚪ 1. Associate an IPv6 CIDR Block with the VPC and Subnets2. Update the Route Tables3. Update the Security Group Rules4. Assign IPv6 Addresses to the EC2 Instance5. Configure the instance to use DHCPv6
Explanation:-The options sequence is incorrect.

Q3)

A tech consultancy company is migrating its applications and data from on-premises to the AWS Cloud. There is a total of 80 TB of data that need to be moved to an S3 bucket in a timely and cost-effective manner.

You estimated that it takes more than one week to upload your data to AWS using the spare capacity of your existing Internet connection.
In this scenario, what is the fastest and the most cost-effective way to migrate the data to AWS?

⚪ Launch a File Gateway using the AWS Storage Gateway service and facilitate an on-premises copy using the file gateway mount point.
Explanation:-This option is incorrect because AWS Storage Gateway is primarily used to augment your on-premises storage capacity and not for migration. In addition, it would still take a lot of time to move 80TB of data using your Internet connection.
⚪ Use multiple Snowball appliances.
Explanation:-This option is incorrect because although a regular Snowball appliance is cheaper than Snowball Edge, it only has a usable capacity of 72 TB (for a regular Snowball 80TB appliance). Hence, you have to order another Snowball appliance to be able to transfer the data to AWS Cloud, which will add to your cost, compared with just using a single Snowball Edge device.
✅ Use a single Snowball Edge appliance.
Explanation:-Snowball is a strong choice for data transfer if you need to more securely and quickly transfer terabytes to many petabytes of data to AWS. Snowball can also be the right choice if you don't want to make expensive upgrades to your network infrastructure, if you frequently experience large backlogs of data, if you're located in a physically isolated environment, or if you're in an area where high-speed Internet connections are not available or cost prohibitive.
As a rule of thumb, if it take
⚪ Use Amazon S3 Transfer Acceleration to migrate the data from the on-premises network to the destination S3 bucket.
Explanation:-This option is incorrect because as mentioned in the scenario, it would take more than one week to upload your data to AWS using the spare capacity of your existing Internet connection. Hence, this approach is not the optimal way to transfer your data. You have to use Snowball in this situation.

Q4) You are managing the deployment process of your applications using CloudFormation where you regularly update the templates to map the latest AMI IDs. Since it takes time to do this all the time, you are looking for ways to streamline and automate this process.
Which of the following should you implement in this scenario?

⚪ Integrate AWS Service Catalog with AWS Config to automatically fetch the latest AMI and use it for succeeding deployments.
Explanation:-This options is incorrect.
⚪ Integrate CloudFormation with Systems Manager State Manager to retrieve the latest AMI IDs for your template. Call the update-stack API in

CloudFormation whenever you decide to update the EC2 instances in your CloudFormation template.
Explanation:-This option is incorrect because the Systems Manager State Manager service simply automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define. This can't be used as a parameter store that refers to the latest AMI of your application.
Integrate AWS Service Catalog with CloudFormation to automatically fetch the latest AMI and use it for succeeding deployments.
Explanation:-This option is incorrect because using AWS Service Catalog is not suitable in this scenario. This service just allows organizations to create and manage catalogs of IT services that are approved for use on AWS.
Integrate CloudFormation with Systems Manager Parameter Store to retrieve the latest AMI IDs for your template. Call the update-stack API in CloudFormation whenever you decide to update the EC2 instances in your CloudFormation template.
Explanation:-You can use the existing Parameters section of your CloudFormation template to define Systems Manager parameters, along with other parameters. Systems Manager parameters are a unique type that is different from existing parameters because they refer to actual values in the Parameter Store. The value for this type of parameter would be the Systems Manager (SSM) parameter key instead of a string or other value. CloudFormation will fetch values stored against these keys in Systems Manager in your a

---

Q5) You are the SysOps Administrator of a leading commercial bank and you discovered an issue on their online banking system which is hosted on their Auto Scaling group, and which has scaled out to over 60 EC2 instances. The Auto Scaling group is taking multiple nodes offline at the same time whenever you update the Launch Configuration. To update the system, the development team decided to use AWS CloudFormation by changing a parameter to the latest version of code.
What can you do to limit the impact on customers while the update is being performed?

Configure the user data script to run the aws ec2 terminate-instances against the next oldest Instance ID.
Explanation:-Use the UpdatePolicy attribute to specify how AWS CloudFormation handles updates to the AWS::AutoScaling::AutoScalingGroup or AWS::Lambda::Alias resource.
For AWS::AutoScaling::AutoScalingGroup resources, AWS CloudFormation invokes one of three update policies depending on the type of change you make or whether a scheduled action is associated with the Auto Scaling group.
1. The AutoScalingReplacingUpdate and AutoScalingRollingUpdate policies apply only when you do one or more of the f
Re-configure the Auto Scaling group to use 6 target groups with 10 EC2 instances each to easily manage the service.
Explanation:-This option is incorrect.
In the CloudFormation template, add the UpdatePolicy attribute and then enable the WaitOnResourceSignals property. In the user data script, append a health check to signal CloudFormation that the update has been successfully completed.
Explanation:-This option is incorrect.
In the CloudFormation template, add a DependsOn attribute to the Auto Scaling group resource to depend on the Launch Configuration. Edit the user data script for each EC2 instance to signal the Wait condition.
Explanation:-This option is incorrect.

Q6) A trade finance application uses AWS Lambda, API Gateway, and Aurora database to process corporate financial transactions such as letters of credit, factoring, and accruals. A new version of their application is ready to be pushed to production using AWS CodeDeploy as the deployment service. You have to specify a percentage of traffic to be shifted to your updated Lambda function version before totally shifting the remaining traffic, so you can do your post verification tests to ensure a smooth deployment.
In this scenario, which is the most suitable configuration type that you should use?

All-at-once
Explanation:-This option is incorrect.
Linear
Explanation:-This option is incorrect.
Canary
Explanation:-If you're using the AWS Lambda compute platform, you must choose one of the following deployment configuration types to specify how traffic is shifted from the original AWS Lambda function version to the new AWS Lambda function version:
-Canary: Traffic is shifted in two increments. You can choose from predefined canary options that specify the percentage of traffic shifted to your updated Lambda function version in the first increment and the interval, in minutes, before the remaining traf
Blue/Green deployment
Explanation:-This option is incorrect.

Q7) You are working as a Systems Administrator for a media startup which has a group of developers that created a photo editing application and hosted it on a large On-Demand EC2 instance. The application allows users to add effects and filters to their photos which are then stored as a media file to an S3 bucket.
Which of the following services will help you build a scalable and decoupled architecture in AWS for this application?

AWS SQS
Explanation:-Amazon Simple Queue Service (SQS) is a fast, reliable, scalable, fully managed message queuing service that lets you easily decouple the components of a cloud application. You can use Amazon SQS to transmit any volume data, without losing messages or requiring other services to be always available. Using SQS on this scenario, the data can be temporarily saved on the SQS queue while the EC2 instances pull the data from the queue and process them. This setup is highly scalable.
AWS STS
Explanation:-This option is incorrect because STS is a web service that is used for requesting temporary tokens to authenticate users.
AWS Elastic Transcoder
Explanation:-This option is incorrect because Elastic Transcoder is used for transcoding video files into different formats.
AWS Glacier
Explanation:-This option is incorrect because Glacier is a service that is used as a low cost storage solution suitable for archiving data.

Q8) You have recently patched your mobile game to a new version, and this was done to attract new players to come and play. Some event contents such as character sprites and items won't be accessible to the new players anymore, but old players who have acquired them before will still be able to use them. Based on the user statistics you have gathered, a bunch of old players are leaving the game each month while a lot of new players are coming in every 2 months.
How should you manage the lifecycle of your content which are stored in S3?

Transfer all event content to an S3-RRS bucket, then configure S3 to delete them after the expiration period passes to save costs.
Explanation:-THis option is incorrect because S3-RRS is designed for non-critical, reproducible data that can be stored with less redundancy, which affects durability of your storage. You might also need the content in the future, so deleting them might not be the best way to go unless you

are sure that you won't need it anymore.
- Create an alarm that checks on player statistics frequently. If there are no old users left, trigger function to transition to Glacier.

Explanation:-This option is incorrect because you need to set up a lifecycle policy and not set up a custom trigger.
- Create a lifecycle policy that transitions to S3-IA after 3 months, and to Glacier after 6 months.

Explanation:-This option is incorrect because you are estimating the lifecycle period. For example, there might be cases when your content are still being accessed frequently after 3 months, or the content are not being accessed anymore after just a month.
- ✅ Use S3 analytics to analyze storage access patterns. When content access is minimal, transition to S3-IA. Then create a lifecycle policy to transition to Glacier.

Explanation:-S3 analytics is a useful tool for analyzing storage access patterns to help you determine when to transition less frequently accessed Standard storage to the IA storage class. Once you see the access patterns in the data, you can then set a lifecycle policy which will transfer the contents to Glacier.

Q9) An Augmented Reality (AR) gaming company currently has three VPC's in the us-east-1 region namely: VPC Alpha, VPC Bravo and VPC Charlie. You are instructed to ensure that all Reserved EC2 instances in all VPC's can communicate with each other.
Which of the following options should you implement to satisfy the given requirement? (Choose 3)

- ✅ Ensure that the three VPCs do not have matching or overlapping IPv4 CIDR blocks.

Explanation:-You may want to use a full mesh configuration when you have separate VPCs that need to share resources with each other without restrictions. In this setup, you have to peer the three VPCs together in which VPC Alpha is peered to VPC Bravo; VPC Alpha is peered to VPC Charlie and lastly, VPC Bravo is peered to VPC Charlie.
- ✅ Ensure that all route tables in each VPC is updated with the respective peering configuration.

Explanation:-You may want to use a full mesh configuration when you have separate VPCs that need to share resources with each other without restrictions. In this setup, you have to peer the three VPCs together in which VPC Alpha is peered to VPC Bravo; VPC Alpha is peered to VPC Charlie and lastly, VPC Bravo is peered to VPC Charlie.
- Set up VPC Peering for all three VPCs with Edge to Edge Routing.

Explanation:-This option is incorrect because Transitive Peering and Edge to Edge Routing are not supported in VPC Peering.
- Set up a Transitive VPC Peering for all three VPCs.

Explanation:-This option is incorrect because Transitive Peering and Edge to Edge Routing are not supported in VPC Peering.
- Set up a VPC Peering with a 'flying V' configuration for all three VPCs in which you have a VPC peering connection between VPC Alpha and VPC Bravo, and between VPC Alpha and VPC Charlie.

Explanation:-This option is incorrect because a 'flying V' configuration only connects VPC Alpha with VPC Bravo, and VPC Alpha with VPC Charlie. This means that there is no connection between VPC Bravo and VPC Charlie hence, the EC2 instances in these two VPC's would not be able to communicate.
- ✅ Set up a VPC Peering with a 'full mesh' configuration for all three VPCs.

Explanation:-You may want to use a full mesh configuration when you have separate VPCs that need to share resources with each other without restrictions. In this setup, you have to peer the three VPCs together in which VPC Alpha is peered to VPC Bravo; VPC Alpha is peered to VPC Charlie and lastly, VPC Bravo is peered to VPC Charlie.

Q10) A leading financial firm is planning to host their new online accounting application in AWS which should support IPv6 address. As their SysOps Administrator, you set up a virtual private cloud (VPC) with a single public subnet and an Internet gateway to enable communication over the Internet.
Which of these options is not needed to satisfy the given requirement?

- Route table entries in the custom route table that enable instances in the VPC to use IPv6 to communicate with each other, and directly over the Internet.

Explanation:-This option is incorrect.
- ✅ Launch an egress-only Internet gateway

Explanation:-For an EC2 instance to be able to communicate to the Internet over IPv6, the following configuration should be done in the VPC:
-Associate a /56 IPv6 CIDR block with the VPC. The size of the IPv6 CIDR block is fixed (/56) and the range of IPv6 addresses is automatically allocated from Amazon's pool of IPv6 addresses (you cannot select the range yourself).
-Create a subnet with a /64 IPv6 CIDR block in your VPC. The size of the IPv6 CIDR block is fixed (/64).
-Create a custom route
- A size /64 IPv6 CIDR block associated with the public subnet

Explanation:-This option is incorrect.
- A size /56 IPv6 CIDR block associated with the VPC

Explanation:-This option is incorrect.

Q11) You recently finished setting up a new virtual private cloud with a size of /16 IPv4 CIDR block including one subnet with a size /24 IPv4 CIDR block in AWS. You also launched an On-Demand EC2 instance, with an NGINX AMI from the AWS Marketplace, which will be used to host the WordPress website of your company. The security group of the instance has also been modified to enable inbound traffic from port 22 to allow you to connect to it using SSH. You attempt to connect to the instance but you failed to establish a connection so you added an Internet Gateway (igw-1a2b3c4d) in your VPC yet, the problem still persists. The main route table has two entries as shown below:
DESTINATION TARGET
http://10.0.0.0/16 local
http://10.0.0.0/16 igw-1a2b3c4d
Which of the following options can you do to solve this issue?

- Attach a NAT gateway to the VPC

Explanation:-This option is incorrect because the NAT gateway is used for EC2 instances hosted in a private subnet to communicate with the Internet.
- Attach an Elastic IP to the Instance

Explanation:-This option is incorrect because even if you have an Elastic IP, the issue will still persist since your Internet Gateway entry in the route table is incorrect.
- ✅ Change the destination of the IGW to 0.0.0.0/0

Explanation:-The first entry is the default entry for local IPv4 routing in the VPC; this entry enables the instances in this VPC to communicate with each other. The second entry routes all other IPv4 subnet traffic to the Internet gateway (igw-1a2b3c4d) which should have a value of 0.0.0.0/0 for its destination.
- Change the destination of the local target to 0.0.0.0/0

Explanation:-This option is incorrect because the local target, which pertains to your VPC, is already correct. You have to change the IGW instead of the local target entry.

Q12)

A leading US-based 24/7 online news network is planning to expand its reach and launch its paid news subscription in Europe, Asia and Oceania regions.

You are instructed to implement multi-region AWS deployments for all their cloud infrastructure where their online platform is hosted.

In this scenario, which Amazon Route 53 feature would minimize response time of their platform for its subscribers?

- Geolocation routing

Explanation:-This option is incorrect.

- Weighted routing policy

Explanation:-This option is incorrect.

- Geoproximity routing policy

Explanation:-This option is incorrect.

- ✅ Latency-based routing

Explanation:-If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.
To use latency-based routing, you create latency records for your resources in multiple AWS Regions. When Route 53 receives a DNS query for your domain or subdomain (example.com or apex.example.com), it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest

---

Q13) A leading energy company is trying to establish a static VPN connection between an on-premises network and their VPC in AWS. As their SysOps Administrator, you created the required virtual private gateway, customer gateway and the VPN connection, including the router configuration on the customer side. Although the VPN connection status seems okay in the console, the connection is not entirely working when you connect to an EC2 instance in their VPC from one of the on-premises virtual machines.
How can you resolve this issue?

- Add a Customer Gateway (CGW) route with the destination of your on-premises network in the route table.

Explanation:-This option is incorrect.

- Create a VPC endpoint.

Explanation:-This option is incorrect.

- Add an Internet gateway (IGW) route with a destination of 0.0.0.0/0 for IPv4 traffic or ::/0 for IPv6 traffic in the route table.

Explanation:-This option is incorrect.

- ✅ Add a Virtual Private Gateway (VGW) route with the destination of your on-premises network in the route table.

Explanation:-To enable instances in your VPC to reach your customer gateway, you must configure your route table to include the routes used by your VPN connection and point them to your virtual private gateway. You can enable route propagation for your route table to automatically propagate those routes to the table for you.
For static routing, the static IP prefixes that you specify for your VPN configuration are propagated to the route table when the status of the VPN connection is UP. Similarly, for

---

Q14) A company has a requirement to connect their on-premises network to a new VPC on AWS to complete their hybrid cloud architecture. As the SysOps Administrator of the company, you are responsible in both managing their cloud infrastructure as well as establishing connectivity to their other corporate data centers.
Which of the following should provide your resources on AWS the connectivity to external networks? (Choose 2)

- Enable AWS enhanced networking on your instances

Explanation:-This option is incorrect because this is used to provide high-performance networking capabilities such as higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. This is not used for providing connectivity to external networks.

- Create additional ENI for the dedicated connection to the on-premises network

Explanation:-This option is incorrect because additional Elastic Network Interface (ENI) on your EC2 will just add another network interface to your instances. With an Internet gateway or VPG, even the default ENI on your instances is enough to provide connectivity.

- ✅ Create a Virtual Private Gateway

Explanation:-This option is the correct answers.
The Internet gateway is used in AWS to connect your VPC to the outside world, the Internet. This is shown in the below diagram as AWS documentation. Only one Internet gateway can be assigned per VPC. The virtual private gateway is used to connect via VPN connection to your on-premises area. This is shown in the below diagram as per AWS documentation. This provides connectivity between an external network to your AWS VPC including those inside the Private

- ✅ Assign an Internet Gateway to the VPC

Explanation:-This option is the correct answers.
The Internet gateway is used in AWS to connect your VPC to the outside world, the Internet. This is shown in the below diagram as AWS documentation. Only one Internet gateway can be assigned per VPC. The virtual private gateway is used to connect via VPN connection to your on-premises area. This is shown in the below diagram as per AWS documentation. This provides connectivity between an external network to your AWS VPC including those inside the Private

- Assign a Public IP to your EC2 instances

Explanation:-This option is incorrect - just like Elastic IP, this will not allow you to connect to external networks without an Internet gateway.

- Assign an Elastic IP to your EC2 instances

Explanation:-This option is incorrect because having an Elastic IP on your instance will not guarantee connectivity to external network. You will still need Internet gateway to send traffic to the external network.

Q15) A media organization recently adopted a hybrid cloud architecture to save costs and to avail of the various AWS cloud products. They have a public website which is deployed to two AWS regions: US East (Ohio) and Asia Pacific (Tokyo), to improve their services in Asia.
As a SysOps Administrator, which of the following should you implement to ensure that users are consistently directed to the

AWS region nearest to them?

Set up the Application Load Balancer of the website to route the incoming traffic to the nearest AWS Region based on its country.
Explanation:-This option is incorrect.
Set up a Route 53 Geoproximity routing policy to direct users in Asia to their website.
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.
To use geoproximity routing, you must use Route 53 traffic flow. You create geoproximity rules for your resources and specify one o
Use a third-party geolocation service and redirect the users to the nearest AWS Region based on their country.
Explanation:-This option is incorrect.
Set up to a Route 53 Latency-based routing for the website.
Explanation:-This option is incorrect.

Q16) A digital advertising company is planning to migrate its web-based data analytics application from its on-premises data center to AWS. You designed the architecture to use an Application Load Balancer and an Auto Scaling group of On-Demand EC2 Instances which are deployed on a private subnet. The instances will be fetching data analytics from various API services over the Internet every 5 minutes. For security reasons, the EC2 instances should not allow any connections initiated from the Internet.
Which of the following options is the most scalable and highly available solution which should be implemented?

Set up a NAT Instance in the private subnet.
Explanation:-This option is incorrect.
Set up a NAT Instance in the public subnet.
Explanation:-This option is incorrect.
Set up a NAT Gateway in the private subnet.
Explanation:-This option is incorrect.
Set up a NAT Gateway in the public subnet.
Explanation:-You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances.
To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. After you've created a NAT gateway, you must update the route table associa

---

Q17) You are working as a Systems Administrator for a technology consulting company where you have been tasked to launch an RDS-MySQL Instance that will host a heavily used relational database. Manual snapshots of the database are done on schedule when the company conducts their disaster recovery activities. To meet the strict compliance requirement, you have to ensure that there are no outages when a snapshot is being created for the database.
Which of the following options is the best way to accomplish this?

Use Provisioned IOPS for the underlying volume type of the RDS instance.
Explanation:-This option is incorrect. Snapshot on a single-AZ can still temporarily suspend I/O operations even with faster disk speeds.
Create a Read Replica of the primary RDS database and take the snapshot from the replica.
Explanation:-This option is incorrect. Although this can help mitigate the I/O suspension, a heavily used database can have many changes in a short amount of time and snapshots taken from read replicas may not include all the transactions present on the master at that time because of possible replica lag.
Generate the DB snapshot during the maintenance window only.
Explanation:-This option is incorrect since this would still result in an scheduled outage.
Re-design the RDS instance to use Multi-AZ deployments configuration.
Explanation:-This is stated in the AWS documentation: Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. Creating this DB snapshot on a Single-AZ DB instance results in a brief I/O suspension that can last from a few seconds to a few minutes, depending on the size and class of your DB instance. Multi-AZ DB instances are not affected by this I/O suspension since the backup is taken on the standby.

Q18) A global news website is deployed in AWS which uses an Application Load Balancer, an Auto Scaling group of On-Demand EC2 instances, and an RDS MySQL Database. Lately, there are a lot of readers that are complaining about the slow loading of the articles in the website. As the Systems Administrator of the company, you analyzed the current architecture and you found that there is a high number of read operations in the database which affects the website's performance.
Which of the following options would you consider to resolve the issue in a cost-effective manner?

Use Automated Backups.
Explanation:-This option is incorrect because Automated Backups is mainly used to recover failed databases.
Change the RDS instance to use Multi-AZ deployments.
Explanation:-This option is incorrect because Multi-AZ deployments is mainly used to provide high availability to the database.
Launch a large ElastiCache instance to work as a database cache for RDS.
Explanation:-This option is incorrect because launching a large ElastiCache instance is expensive compared to Read Replicas.
Use Read Replicas.
Explanation:-Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalo

---

Q19) A document management system which is hosted in AWS uses an S3 bucket to store its data. Due to a recent cyber attack, the IT Security department mandated that all objects must be encrypted at rest.
Which of the following is a valid option to use to fulfill this requirement? (Choose 3)

Use AWS server-side encryption for the S3 bucket with Customer-Provided Keys.
Explanation:-Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a presigned URL, that

URL works the same way for both encrypted and unencrypted objects.
You h
○ Use the Access Control List (ACL) of the bucket to encrypt all objects in the S3 bucket.
Explanation:-This option is incorrect.
○ Use the S3 Bucket Policy to automatically encrypt all objects.
Explanation:-This option is incorrect.
✓ Use AWS server-side encryption for the S3 bucket with AWS KMS Keys.
Explanation:-Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a presigned URL, that URL works the same way for both encrypted and unencrypted objects.
You h
✓ Use AWS server-side encryption for the S3 bucket with AWS Managed Keys.
Explanation:-Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a presigned URL, that URL works the same way for both encrypted and unencrypted objects.
You h
○ Enable CORS in the S3 bucket.
Explanation:-This option is incorrect.

Q20)

You launched an EBS-backed On-Demand EC2 Instance to host a web application. However, the instance always terminates after going into the pending state.

Which of the following could be the cause of this issue? (Choose 3)

✓ AWS does not currently have enough available On-Demand capacity to service your request.
Explanation:-The following are a few reasons why your EC2 instance goes from the pending state to the terminated state immediately after restarting it:
You've reached your EBS volume limit. An EBS snapshot is corrupt.
The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.
The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file).
○ The EBS snapshot from which the instance is being launched is corrupt.
Explanation:-This option is incorrect.
✓ The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.
Explanation:-The following are a few reasons why your EC2 instance goes from the pending state to the terminated state immediately after restarting it:
You've reached your EBS volume limit. An EBS snapshot is corrupt.
The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.
The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file).
○ The limit for EC2 Instances in your region has already been reached.
Explanation:-This option is incorrect.
✓ The EBS volume limit has been reached.
Explanation:-The following are a few reasons why your EC2 instance goes from the pending state to the terminated state immediately after restarting it:
You've reached your EBS volume limit. An EBS snapshot is corrupt.
The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.
The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file).
○ The AMI used is corrupted.
Explanation:-This option is incorrect.

Q21) A popular online graphic design tool startup uses a standard S3 bucket that has versioning enabled to store the user-generated images on its platform. They have millions of users around the globe that store their logos, graphics, infographics, and other designs on their platform. Lately, there are a lot of users complaining that they receive a lot of HTTP 503 responses on the platform.
Which of the following options could be the reason why this issue exists?

○ The Cross-Region Replication (CRR) option is not enabled, which is required if the S3 bucket is being accessed from multiple regions.
Explanation:-This option is incorrect.
○ S3 could not handle simultaneous access to the bucket since the S3 transfer acceleration option is not enabled.
Explanation:-This option is incorrect.
○ The cross-origin resource sharing (CORS) option is not enabled.
Explanation:-This option is incorrect.
✓ You might have one or more objects in the bucket for which there are millions of versions.
Explanation:-If you notice a significant increase in the number of HTTP 503-slow down responses received for Amazon S3 PUT or DELETE object requests to a bucket that has versioning enabled, you might have one or more objects in the bucket for which there are millions of versions. When you have objects with millions of versions, Amazon S3 automatically throttles requests to the bucket to protect the customer from an excessive amount of request traffic, which could potentially impede other requests made to the

---

Q22) As part of the yearly AWS data cleanup, you need to delete all unused S3 buckets and their contents. The tutorialsdojo bucket, which contains several educational video files, has both the Versioning and MFA Delete features enabled. One of your Systems Engineers who has an Administrator account tried to delete an S3 bucket using the aws s3 rb s3://tutorialsdojo command. However, the operation fails even after repeated attempts.
Which of the following options should you do to properly delete the bucket? (Choose 2)

✓ Have the root account owner suspend MFA and versioning in the bucket. Configure a lifecycle rule to expire current object versions and permanently remove non-current object versions. Permanently purge all objects and delete markers then delete your bucket again.
Explanation:-You can delete a bucket that contains objects using the AWS CLI only if the bucket does not have versioning enabled. If your bucket

does not have versioning enabled, you can use the rb (remove bucket) AWS CLI command with --force parameter to remove a non-empty bucket. An IAM Administrator account can suspend Versioning on an S3 bucket but only the bucket owner can enable/suspend the MFA-Delete on the objects. You can configure lifecycle on your bucket to expire objects and request that Ama

○ Delete all markers from the S3 bucket and then run the aws s3 rb s3://tutorialsdojo command again to fully delete the bucket and its contents.

Explanation:-This option is incorrect because although it is correct to remove all of the delete markers, you still need to remove all current and non-current objects before the S3 bucket can be deleted.

✓ Remove the policy that requires MFA Delete on your S3 bucket. Use the AWS SDK to remove all of the bucket's delete markers and object versions. Delete the bucket again using the same CLI command that you used before.

Explanation:-You can delete a bucket that contains objects using the AWS CLI only if the bucket does not have versioning enabled. If your bucket does not have versioning enabled, you can use the rb (remove bucket) AWS CLI command with --force parameter to remove a non-empty bucket. An IAM Administrator account can suspend Versioning on an S3 bucket but only the bucket owner can enable/suspend the MFA-Delete on the objects. You can configure lifecycle on your bucket to expire objects and request that Ama

○ Use the aws s3 rb s3://tutorialsdojo command again with an additional --force option to forcibly delete the bucket via the CLI.

Explanation:-This options is incorrect because you can only use the --force parameter to delete a non-empty bucket if the versioning feature is disabled.

○ Use the AWS SDK to send deletion requests to S3 to remove all objects in your bucket. Ensure that you include the x-amz-mfa header in all requests which contains the MFA authentication code. Afterwards, retry to delete the bucket with the same CLI command that you used before.

Explanation:-This option is incorrect because although it is correct to use the x-amz-mfa header on your HTTPS requests to delete protected objects, this is still not enough to delete the whole S3 bucket. You will still need to remove all existing delete markers in order for the bucket to be properly deleted.

Q23) The development team of your company is currently working on a web application which uses a NoSQL database. The application has been successfully deployed to the production environment including a DynamoDB table. Now, there is a new requirement for users in another AWS region to access the data in the DynamoDB table.
Which of the following options can be used to ensure that the data can be accessed in the other region with the least latency?

○ Set up an Auto Scaling group of DynamoDB instances.

Explanation:-This option is incorrect because the Auto Scaling group is mainly used for EC2 instances and not for DynamoDB.

○ Launch Read Replicas.

Explanation:-This option is incorrect because Read Replicas and Multi-AZ deployments are only used for RDS.

○ Configure the database to use Multi-AZ deployments.

Explanation:-This option is incorrect because Read Replicas and Multi-AZ deployments are only used for RDS.

✓ Create a DynamoDB global table.

Explanation:-Amazon DynamoDB global tables provide a fully managed solution for deploying a multi-region, multi-master database, without having to build and maintain your own replication solution. When you create a global table, you specify the AWS regions where you want the table to be available. DynamoDB performs all of the necessary tasks to create identical tables in these regions, and propagate ongoing data changes to all of them.

Q24) You are the Systems Administrator of an investment firm where you are tasked to create a Provisioned IOPS volume in AWS. The size of the volume is 10 GiB.
In this scenario, what is the maximum value that can be put as the IOPS of the volume?

○ 400

Explanation:-This option is incorrect because although a value of 400 is an acceptable value, it is not the maximum value for the IOPS. You will not fully utilize the available IOPS that the volume can offer if you just set it to 400.

✓ 500

Explanation:-Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year.
An io1 volume can range i

○ 600

Explanation:- This option is incorrect because the maximum IOPS for the 10 GiB volume is only 500. Therefore, any value greater than the maximum amount, such as 600 or 800, is wrong.

○ 800

Explanation:- This option is incorrect because the maximum IOPS for the 10 GiB volume is only 500. Therefore, any value greater than the maximum amount, such as 600 or 800, is wrong.

Q25) AWS regularly releases service updates and changes to constantly improve its entire global architecture that might affect your cloud resources. To ensure the continuous flow of your business, you need to be immediately notified for any outages or any underlying infrastructure changes that AWS has made.
Which of the following services can help you in this scenario?

○ AWS IAM

✓ AWS Personal Health Dashboard

Explanation:-AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources. The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by ch

○ AWS Trusted Advisor

○ AWS Billing Dashboard

Q26) You are working as a Systems Administrator for an IT Consulting firm where you are responsible for monitoring and managing organizational costs and financial matters of their cloud infrastructure. Additionally, you will also be producing reports for your superiors to constantly inform them of the operational expenses.
In AWS, what is the best way to generate reports that would provide insight into service usage and costs as you deploy and operate your cloud architecture?

○ Use the information in AWS Pricing page

Explanation:-The Cost Optimization Monitor can help you generate reports that provide insight into service usage and costs as you deploy and operate cloud architecture. They include detailed billing reports, which you can access in the AWS Billing and Cost Management console. These reports provide estimated costs to help monitor and forecast monthly charges. You can analyze this information to optimize your infrastructure and maximize your return on investment using elasticity. The solution uses Amazon Elast

- Use the AWS Simple Monthly Calculator

Explanation:-The Cost Optimization Monitor can help you generate reports that provide insight into service usage and costs as you deploy and operate cloud architecture. They include detailed billing reports, which you can access in the AWS Billing and Cost Management console. These reports provide estimated costs to help monitor and forecast monthly charges. You can analyze this information to optimize your infrastructure and maximize your return on investment using elasticity. The solution uses Amazon Elast

- Use the AWS TCO calculator

Explanation:-The Cost Optimization Monitor can help you generate reports that provide insight into service usage and costs as you deploy and operate cloud architecture. They include detailed billing reports, which you can access in the AWS Billing and Cost Management console. These reports provide estimated costs to help monitor and forecast monthly charges. You can analyze this information to optimize your infrastructure and maximize your return on investment using elasticity. The solution uses Amazon Elast

- ✅ Use the Cost Optimization Monitor

Explanation:-The Cost Optimization Monitor can help you generate reports that provide insight into service usage and costs as you deploy and operate cloud architecture. They include detailed billing reports, which you can access in the AWS Billing and Cost Management console. These reports provide estimated costs to help monitor and forecast monthly charges. You can analyze this information to optimize your infrastructure and maximize your return on investment using elasticity. The solution uses Amazon Elast

---

Q27) A social media company has hired a SysOps Administrator to ensure that all of their CloudFormation stacks use the latest Windows AMI. The solution should have a minimal management overhead as they would need to update their Windows AMI again to get the latest security patches in the future.
Which is the most suitable option that will meet the requirement?

- Develop a REST API which gets the latest Windows AMI and update the CloudFormation template. Update the template again if the ImageID changes.

Explanation:-This option is incorrect because developing a brand new REST API entails a lot of effort and time to execute. Simply using AWS Systems Manager Parameter Store with CloudFormation should suffice.

- Using SNS, get all the latest updates from Windows AMI notifications. Launch an AWS Lambda function which updates to the CloudFormation template and set a trigger to run the function when a new AMI is released.

Explanation:-This option is incorrect because although this solution could work, using Windows AMI notifications and a Lambda function to simply track the AMI ID entails high operational overhead since you will have to build and maintain these systems. The best way in this scenario is to configure the CloudFormation template to just refer to AWS Systems Manager Parameter Store to get the updated AMI ID, rather than regularly updating the templates using a Lambda function.

- Modify all of their CloudFormation templates to use the latest Windows AMI. Just update the CloudFormation template once again when new AMIs are released.

Explanation:-This option is incorrect because manually updating the CloudFormation template has a high operational overhead and doesn't automate the process.

- ✅ Use AWS Systems Manager to achieve this task. Configure the Parameters section in the template to specify the latest version of Windows regional AMI ID.

Explanation:-WS Systems Manager allows you to automate operational actions to help make your teams more efficient. You can automate maintenance and deployment tasks on Amazon EC2 and on-premises instances, or automatically apply patches, updates, and configuration changes across any resource group. Systems Manager provides predefined automation documents for common operational tasks, such as stopping and restarting an EC2 instance, that you can customize to your own specific use cases. Systems Manager also h

---

Q28) You are working as an IT Consultant for a leading pharmaceutical company which has a hybrid cloud architecture. The company has a fleet of EC2 instances in their VPC and a group of servers on their on-premises data center. You are instructed by your manager to set up a unified dashboard monitoring system for both the EC2 instances as well as the on-premises servers.
Which of the following options should you do to satisfy the given requirement? (Choose 4)

- ✅ Create the IAM roles and users that you need for the CloudWatch agent.

Explanation:-To collect metrics and logs on both Amazon EC2 Instances and On-Premises Servers, you can install a unified CloudWatch agent which enables you to do the following:
-Collect more system-level metrics from Amazon EC2 instances, including in-guest metrics. -Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS. -Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows

- ✅ Install the CloudWatch Agent to the Amazon EC2 Instances only. Set up a custom monitoring tool for the On-Premises servers that publishes metrics to CloudWatch in real-time.

Explanation:-To collect metrics and logs on both Amazon EC2 Instances and On-Premises Servers, you can install a unified CloudWatch agent which enables you to do the following:
-Collect more system-level metrics from Amazon EC2 instances, including in-guest metrics. -Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS. -Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows

- Install the CloudWatch Agent to both Amazon EC2 Instances and On-Premises servers.

Explanation:-This option is incorrect because you have to install the CloudWatch agent on both the EC2 instances in your VPC as well as the servers located in your data center.

- ✅ Set up the metrics dashboard in CloudWatch.

Explanation:-To collect metrics and logs on both Amazon EC2 Instances and On-Premises Servers, you can install a unified CloudWatch agent which enables you to do the following:
-Collect more system-level metrics from Amazon EC2 instances, including in-guest metrics. -Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS. -Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows

- Enable CloudTrail Event History for the EC2 instances.

Explanation:-This option is incorrect because you do not need to use CloudTrail in this scenario. This is only used to get the API logs of the AWS resources that you are using.

- ✅ Create the CloudWatch Agent Configuration File.

Explanation:-To collect metrics and logs on both Amazon EC2 Instances and On-Premises Servers, you can install a unified CloudWatch agent which enables you to do the following:

-Collect more system-level metrics from Amazon EC2 instances, including in-guest metrics. -Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS. -Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows

---

Q29) A university has a web-based learning management system hosted on its on-premises data center that they want to migrate to their AWS Cloud. Due to the volume of local and overseas students that use their system, they need to deploy up to 60 c3.4xlarge EC2 instances on their VPC.
As the SysOps Administrator, what should you do prior to the migration?

- Do nothing. You can directly launch 60 c3.4xlarge EC2 instances in AWS at the same time.

Explanation:-This option is incorrect.

- Use the AWS Trusted Advisor to increase the default service limits for EC2 instances.

Explanation:-This option is incorrect.

- ✅ Create a case in the AWS Support Center page and request for a service limit increase.

Explanation:-By default, there is an imposed limit in launching EC2 instances in your VPC. These increases are not granted immediately, so it may take a couple of days for your increase to become effective. To request a limit increase:
Open the AWS Support Center page, sign in if necessary, and choose Create case. For Regarding, choose Service Limit Increase.
Complete the form. If this request is urgent, choose Phone as the method of contact instead of Web.

- Ensure that you have enabled Enhanced Networking and created 60 Elastic IP addresses before launching the EC2 instances.

Explanation:-This option is incorrect.

Q30) You are working as an IT Consultant for a large insurance company. Their accounting system is hosted in AWS, which consists mainly of On-Demand EC2 Instances with an Application Load Balancer in front to distribute the incoming load. The IT Security department needs to conduct a vulnerability analysis on these servers to ensure that the EC2 instances comply with the latest security standards.
In this scenario, which of the following options would you implement to satisfy this requirement?

- AWS CloudFront

Explanation:-This option is incorrect because CloudFront is used as a content distribution service.

- AWS Snowball

Explanation:-This option is incorrect because Snowball is mainly used to transfer data from your on-premises network to AWS.

- AWS WAF

Explanation:-This option is incorrect because AWS WAF is a firewall service to safeguard your VPC against DDoS, SQL Injection, and many other threats.

- ✅ AWS Inspector

Explanation:-Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you to identify potential security issues. Using Amazon Inspector, you can define a collection of AWS resources that you want to include in an assessment target. You can then create an assessment template and launch a security assessment run of this target.

Q31) You are working as the SysOps Administrator of a large technology company which is heavily using AWS for its cloud-based applications to serve their clients. They both have private and public application servers which are hosted in over 1000 EC2 Instances. To ensure security, you need to ensure that public SSH is always disabled for the private servers.
Which of the following options would be the best way to ensure this security check is in place?

- Use the EC2 Config utility to check all the configuration of the Security groups.

Explanation:-This option is incorrect.

- Write a shell script to check all the Security groups in your VPC.

Explanation:-This option is incorrect.

- ✅ Use AWS Config Rules to check all the configuration of the Security Groups.

Explanation:-To analyze potential security weaknesses, you need detailed historical information about your AWS resource configurations, such as the AWS Identity and Access Management (IAM) permissions that are granted to your users, or the Amazon EC2 security group rules that control access to your resources.
You can use AWS Config to view the IAM policy that was assigned to an IAM user, group, or role at any time in which AWS Config was recording. This information can help you determine the permissions

- Use AWS Inspector to check all the configuration of the Security Groups.

Explanation:-This option is incorrect.

Q32) An online tax filing application uses large On-Demand EC2 instances for its front-end tier and an RDS MySQL instance as its database. The Operations team has noticed some issues on the performance of the MySQL database. As the Systems Administrator, you need to see if there are any ways to improve the performance of the database.
Which of the following options can be used for this purpose?

- AWS Config

Explanation:-This option is incorrect because AWS Config is a configuration management utility.

- AWS Inspector

Explanation:-This option is incorrect because AWS Inspector is used as an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

- ✅ AWS Performance Insights

Explanation:-Performance Insights expands on existing Amazon RDS monitoring features to illustrate your database's performance and help you analyze any issues that affect it. With the Performance Insights dashboard, you can visualize the database load and filter the load by waits, SQL statements, hosts, or users. Performance Insights is on by default in the console create wizard for the Amazon Aurora MySQL, Amazon Aurora PostgreSQL, and Amazon RDS PostgreSQL DB engines. If you have more than one database on

- AWS Trusted Advisor

Explanation:-This option is incorrect because AWS Trusted Advisor cannot give you a thorough analysis on the database issues.

Q33) You are working as a SysOps Administrator for a large investment bank which has an online stock trading platform deployed in AWS. The trading platform is hosted in an Auto Scaling group of EC2 instances with an Application Load Balancer in front to evenly distribute the load. For security compliance, the IT Security department needs to be able to view the IP address of the incoming traffic.

Which of the following options can be used to meet the requirement?

✅ Use AWS VPC Flow Logs
Explanation:-VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.
Flow logs can help you with a number of tasks; for example, to troubleshoot why specific traffic is not reaching an instance, which in turn helps you diagnose overly restrictive security gro

⚪ Use AWS Inspector
Explanation:-This option is incorrect because AWS Inspector is just an automated security assessment service that helps you test the security state of your applications running on Amazon EC2. It could not provide the list of incoming IP addresses accessing the EC2 instance.

⚪ Use CloudTrail logs
Explanation:-This option is incorrect because CloudTrail is used for API logging of various AWS resources.

⚪ Use AWS Trusted Advisor
Explanation:-This option is incorrect because AWS Trusted Advisor service can only be used to get recommendations but not make any change in your VPC.

Q34) You are the Systems Administrator for a large insurance firm which heavily uses AWS as its cloud infrastructure. Your manager instructed you to set up a monitoring system to ensure that the operations team can quickly respond to any incidents that may affect the production environment. There should be a dashboard that contains the CPUUtilization, DiskReadOps, NetworkIn and other metrics for all EC2 instances at one-minute intervals.
Which of the following should you do to properly implement this system? (Choose 2)

⚪ Set up an Amazon QuickSight dashboard.
Explanation:-This option is incorrect because Amazon QuickSight is only a business analytics service that you can use to build visualizations, perform ad hoc analysis, and get business insights from your data. This is not a monitoring service.

⚪ Use the AWS Service Health Dashboard.
Explanation:-This option is incorrect because the AWS Service Health Dashboard is mainly used to monitor the health of the entire AWS cloud services and not just your own VPC.

⚪ Set up a dashboard in CloudTrail.
Explanation:-This option is incorrect because CloudTrail is only used for API-based logging of the AWS resources you have used.

✅ Set up a CloudWatch dashboard.
Explanation:-Amazon EC2 sends metrics to Amazon CloudWatch. You can use the AWS Management Console, AWS CLI, or an API to list the metrics that Amazon EC2 sends to CloudWatch. By default, each data point covers the previous 5 minutes of activity for the instance. If you've enabled detailed monitoring, each data point covers the previous 1 minute of activity.
Amazon CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view, eve

⚪ Enable basic monitoring for the EC2 instances in CloudWatch.
Explanation:- This option is incorrect because Basic Monitoring will not meet the requirement of 1-minute interval logging of metrics.

✅ Enable detailed monitoring for the EC2 instances.
Explanation:-Amazon EC2 sends metrics to Amazon CloudWatch. You can use the AWS Management Console, AWS CLI, or an API to list the metrics that Amazon EC2 sends to CloudWatch. By default, each data point covers the previous 5 minutes of activity for the instance. If you've enabled detailed monitoring, each data point covers the previous 1 minute of activity.
Amazon CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view, eve

---

Q35) You have multiple sets of running EC2 instances, with each set having an ELB to distribute traffic among them. It is important that the endpoints are reachable, and you should be notified if something goes wrong. Route 53 health checks integrate with CloudWatch alarms to provide you tools to watch over the health of your endpoints.
Which of the following are valid types of Amazon Route 53 health checks that you can use? (Choose 3)

✅ Health checks that monitor other health checks (calculated health checks)
Explanation:-You can create three types of Amazon Route 53 health checks:
Health checks that monitor an endpoint. You can configure a health check that monitors an endpoint that you specify either by IP address or by domain name. At regular intervals that you specify, Route 53 submits automated requests over the internet to your application, server, or other resource to verify that it's reachable, available, and functional. Optionally, you can configure the health check to make requests similar to those

⚪ Health checks that monitor CloudTrail alarms
Explanation:-This option is incorrect.

✅ Health checks that monitor an endpoint
Explanation:-You can create three types of Amazon Route 53 health checks:
Health checks that monitor an endpoint. You can configure a health check that monitors an endpoint that you specify either by IP address or by domain name. At regular intervals that you specify, Route 53 submits automated requests over the internet to your application, server, or other resource to verify that it's reachable, available, and functional. Optionally, you can configure the health check to make requests similar to those

⚪ Health checks that monitor the AWS Route 53 Service Health from the Service Health Dashboard
Explanation:-This option is incorrect.

⚪ Health checks that monitor the CPU Usage of the EC2 instance
Explanation:-This option is incorrect.

✅ Health checks that monitor CloudWatch alarms
Explanation:-You can create three types of Amazon Route 53 health checks:
Health checks that monitor an endpoint. You can configure a health check that monitors an endpoint that you specify either by IP address or by domain name. At regular intervals that you specify, Route 53 submits automated requests over the internet to your application, server, or other resource to verify that it's reachable, available, and functional. Optionally, you can configure the health check to make requests similar to those

---

Q36) You are instructed to grant a user the ability to pass any of the approved set of roles to the Amazon EC2 service upon launching an instance. This will enable the user to start an EC2 instance with an assigned role. In effect, the applications running on the instance can access temporary credentials for the role through the instance profile metadata.
Which of the following options should you implement together to accomplish this requirement? (Choose 2)

✅ Set up an IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. Use the iam:PassRole

and iam:GetRole permissions in order for the user to get the details of the role to be passed.
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

✅ Set up an IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. Afterwards, create a trust policy for the role that allows the service to assume the role.
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

⚪ Set up an IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. Use the iam:PassedToService and iam:GetRolePolicy permissions in order for the user to get the details of the role to be passed.
Explanation:-This option is incorrect because you have to use iam:PassRole and iam:GetRole permissions in order for user to get the details of the role to be passed. The iam:PassedToService permission is simply a condition key that is used to filter access by the AWS service to which this role is passed. The GetRolePolicy on the other hand, just grants permission to retrieve an inline policy document that is embedded with the specified IAM role.

⚪ Set up a Service Control Policy attached to the IAM user that allows the user to pass only those roles that are approved. Afterwards, create a trust policy for the role that allows the service to assume the role.
Explanation:-This option is incorrect as you have to set up an IAM permissions policy and not a Service Control Policy, and then attach it to the IAM user to allow the user to pass only those roles that are approved.

⚪ Set up an IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. Afterwards, create a Service Control Policy for the role that allows the service to assume the role.
Explanation:-This option is incorrect because you have to create a trust policy, and not a service control policy, for the role that allows the service to assume the role. Service control policies (SCPs) are primarily used in conjunction with AWS Organizations to specify the maximum permissions for member accounts in the organization. Therefore, this is not applicable in this scenario.

Q37) A leading commercial bank is hosting its personal banking portal on a large EC2 instance in AWS. You received a report from your IT Security team that they discovered a lot of SQL injection attempts and cross-site scripting attacks on the online portal.
Which of the following service can help mitigate this attack?

✅ AWS WAF
Explanation:-AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your spec

⚪ Network Access Control Lists
Explanation:-AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your spec

⚪ AWS Autoscaling
Explanation:-AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your spec

⚪ AWS Application Load Balancer
Explanation:-AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your spec

---

Q38) You are part of the IT Operations team of your company that manages a suite of web applications that use a DynamoDB table. You will be using EC2 instances to host the application and will access the newly created DynamoDB table.
Which of the following will you need to do to ensure that the application has the relevant permissions to access the DynamoDB table?

⚪ Create Access Keys with the required permissions to DynamoDB and ensure that the keys are embedded on the application.
Explanation:-This option is incorrect because embedding Access Keys is not a secure way to access AWS resources from EC2 instances. This is not recommended because if someone had accidentally got access to the EC2 instance, then the access key might be seen and exploited.

✅ Create an IAM Role with the required permissions to DynamoDB. Grant the IAM Role to the EC2 instance.
Explanation:-You can refer to the diagram below that provides an example on when to create an IAM role instead of an IAM User. You're creating an application that runs on Amazon Elastic Compute Cloud (Amazon EC2) instance and that application makes requests to AWS.

⚪ Create an IAM group with the required permissions to DynamoDB and ensure the application runs on behalf of the IAM group on the EC2 instance.
Explanation:-This option is incorrect since you need to use IAM roles. These are primarily used for users logging-in on the AWS console.

⚪ Create an IAM User with the required permission to DynamoDB and then attach it to the EC2 instance.
Explanation:-This option is incorrect since you need to use IAM roles. These are primarily used for users logging-in on the AWS console.

Q39) A data analytics company has a dockerized application running in ECS with a DynamoDB database. The IT security team has detected malicious traffic coming from a specific set of IP addresses.
Which of the following should you do to block the incoming traffic from these IP addresses?

⚪ Block the incoming traffic by deploying the ECS instance to a private subnet.
Explanation:-This option is incorrect.

⚪ Block the incoming traffic by setting up a firewall in the ECS instance.

Explanation:-This option is incorrect.

✅ Block the incoming traffic using Network Access Control List.

Explanation:-A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You may set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

⚪ Block the incoming traffic using the Security Group of the ECS instance.

Explanation:-This option is incorrect.

Q40) An artificial intelligence startup that produces AI-powered smart robots was recently acquired by a tech giant for $100 million. Their current AWS setup consists of multiple AWS accounts but due to the acquisition, there is now a requirement to consolidate their accounts into an organization and also have the ability to centrally manage it. As their SysOps Administrator, you should also have the ability to restrict what services and actions the users, groups, and roles in those accounts can do, at the account level of granularity.
How would you achieve the requirement in the most effective way possible?

⚪ Connect all of the VPCs of each AWS account using VPC peering. Set up a Single-Sign On (SSO) authentication in order to centrally manage the accounts.

Explanation:-This option is incorrect.

✅ Use AWS Organizations and Service Control Policies.

Explanation:-AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. AWS Organizations includes consolidated billing and account management capabilities that enable you to better meet the budgetary, security, and compliance needs of your business. As an administrator of an organization, you can create accounts in your organization and invite existing accounts to join the organization.

Service cont

⚪ Connect all AWS Accounts using cross-account access and set up an IAM policy to centrally manage all accounts.

Explanation:-This option is incorrect.

⚪ Configure an IAM policy that can be applied across all AWS accounts.

Explanation:-This option is incorrect.

⚪ Use AWS Organizations and create Organizational Units (OUs).

Q41)

To meet the security compliance requirement, your manager instructed you to set up an ELB with SSL using a security policy for secure negotiation between the client and load balancer.

Which of the following is not a security feature that you can configure in the ELB?

✅ Front-End Server Authentication

Explanation:-You can create a load balancer with the following security features:
-SSL Server Certificates
-SSL Negotiation
-Back-End Server Authentication

⚪ Back-End Server Authentication

Explanation:-This option is incorrect.

⚪ SSL Negotiation

Explanation:-This option is incorrect.

⚪ SSL Server Certificates

Explanation:-This option is incorrect.

Q42) A document management system of a legal firm is hosted in AWS Cloud with an S3 bucket as the primary storage service. To comply with the security requirements, you are instructed to ensure that the confidential documents and files stored in AWS are secured.
Which features can be used to restrict access to data in S3? (Choose 2 options)

⚪ Set up a Single Sign-On feature (SSO) with IAM Identity Federation.

Explanation:-This option is incorrect.

✅ Configure the S3 ACL on the bucket of each individual object.

Explanation:-By default, all Amazon S3 resources—buckets, objects, and related subresources (for example, lifecycle configuration and website configuration)—are private: 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 your resources (buckets

⚪ Enable Cross-region replication (CRR).

Explanation:-This option is incorrect.

✅ Configure the S3 bucket policy to only allow access to authorized personnel.

Explanation:-By default, all Amazon S3 resources—buckets, objects, and related subresources (for example, lifecycle configuration and website configuration)—are private: 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 your resources (buckets

⚪ Launch a CloudFront distribution for the bucket.

Explanation:-This option is incorrect.

⚪ Disable Cross-Origin Resource Sharing (CORS).

Explanation:-This option is incorrect.

Q43)

Your teammate has recently resigned and she handed over a set of CloudFormation templates that she is maintaining to you. You checked the templates and looked at the configured IAM policy for an S3 bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
       ],
        "Resource": "*"
     },
     {
       "Effect": "Allow",
       "Action": "s3:PutObject",
       "Resource": "arn:aws:s3:::tutorialsdojo\/*"
      }
   ]
}
```

What does the following IAM policy allow? (Choose 3 options)

- An IAM user with this IAM policy is allowed to read and delete objects from the 'tutorialsdojo' S3 bucket.

Explanation:-This option is incorrect because although you can read objects from the bucket, you cannot delete any objects.

- An IAM user with this IAM policy is allowed to read objects in the 'tutorialsdojo' S3 bucket but not allowed to list the objects in the bucket.

Explanation:-This option is incorrect it can be clearly seen in the template the there is a s3:Get* which permits the user to list objects.

- ✅ An IAM user with this IAM policy is allowed to read objects from the 'tutorialsdojo' S3 bucket.

Explanation:-Based on the template, the user is only allowed to get, write and list all of the objects for the 'tutorialsdojo' s3 bucket. The s3:PutObject basically means that you can submit a PUT object request to the S3 bucket to store data. Hence, the Options are the correct answers:
* An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.
*An IAM user with this IAM policy is allowed to write objects into the 'tutorialsdojo' S3 bucket.
*An IAM

- An IAM user with this IAM policy is allowed to change access rights for the 'tutorialsdojo' S3 bucket.

Explanation:-This option is incorrect the template does not have any statements which allows the user to change access rights in the bucket.

- ✅ An IAM user with this IAM policy is allowed to write objects into the 'tutorialsdojo' S3 bucket.

Explanation:-Based on the template, the user is only allowed to get, write and list all of the objects for the 'tutorialsdojo' s3 bucket. The s3:PutObject basically means that you can submit a PUT object request to the S3 bucket to store data. Hence, the Options are the correct answers:
* An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.
*An IAM user with this IAM policy is allowed to write objects into the 'tutorialsdojo' S3 bucket.
*An IAM

- ✅ An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.

Explanation:-Based on the template, the user is only allowed to get, write and list all of the objects for the 'tutorialsdojo' s3 bucket. The s3:PutObject basically means that you can submit a PUT object request to the S3 bucket to store data. Hence, the Options are the correct answers:
* An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.
*An IAM user with this IAM policy is allowed to write objects into the 'tutorialsdojo' S3 bucket.
*An IAM

Q44) As the SysOps Administrator, you are responsible for provisioning the required resources and access policies of your cloud infrastructure. You received a request from one of the development teams to be able to create, overwrite, and delete any object in an S3 bucket as well as to write additional ACL for the applicable bucket.
Which bucket ACL permission should you grant?

- FULL_CONTROL

Explanation:-This option is incorrect because although this permission can provide the required WRITE and WRITE_ACP permissions for the team, it will also allow the READ and READ_ACP permissions which are not required. You have to always follow the principle of least privilege when it comes to providing access.

- READ and READ_ACP

Explanation:-This option is incorrect because this will only allow the grantee to list the objects and read the bucket ACL.

- ✅ WRITE and WRITE_ACP

Explanation:-Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify that the requester has the necessary access permissions.
The WRITE ACL permission allows grantee to create, overwrite, and delete any object in the bucket and

- WRITE

Explanation:-This option is incorrect because this permission alone does not allow the grantee to write the ACL for the applicable bucket.

- READ

Explanation:- This option is incorrect because it will only provide read access to the objects of the bucket.

Q45) You are setting up the bucket ACL in S3 to allow users to list all the objects in the tutorialsdojo bucket and retrieve them. You prepared the below policy using the AWS Policy Generator.
What will happen if you apply this bucket policy in S3?

- The tutorialsdojo bucket including all its objects will be publicly visible to anyone but downloading the objects is not allowed.

Explanation:-This option is incorrect.

- The tutorialsdojo bucket including all its objects will be publicly visible to anyone.

Explanation:-This option is incorrect.

- The tutorialsdojo bucket including all its objects will be publicly accessible and downloadable to anyone.

Explanation:-This option is incorrect.

- ✅ You will be prompted with an "Action does not apply to any resource(s) in statement" error.

Explanation:-In this scenario, you will be prompted with an "Action does not apply to any resource(s) in statement" error if you tried to apply this bucket policy. The statement is using the s3:GetObject action, which means that you should add the specific object in the bucket. If this is not

declared, then an error will be thrown.
To fix the policy, you simply have to specify two items under the Resource section: one for the s3:GetObject action and another one for the s3:ListBucket action. Take note th

---

Q46) Due to the upcoming IT security audit, your manager instructed you to encrypt all objects being uploaded to their S3 bucket. You decided to implement a server side encryption by supplying your own encryption key.
Which of the following request headers is not valid when using server-side encryption with customer-provided encryption keys?

- x-amz-server-side-encryption-customer-key

Explanation:-This option is incorrect.

- x-amz-server-side-encryption-customer-algorithm

Explanation:-This option is incorrect.

- x-amz-server-side-encryption-customer-key-MD5

Explanation:-This option is incorrect.

- ✅ x-amz-server-side-encryption

Explanation:-When using server-side encryption with customer-provided encryption keys (SSE-C), you must provide encryption key information using the following request headers:
x-amz-server-side-encryption-customer-algorithm
x-amz-server-side-encryption-customer-key
x-amz-server-side-encryption-customer-key-MD5
Hence, Options 1, 2, 3 are all valid request headers. The x-amz-server-side-encryption is used for Amazon S3-Managed Encryption Keys (SSE-S3) and not for SSE-C.
x-amz-ser

Q47) You are working as an IT Consultant for a large accounting firm that is heavily using AWS. They have a web application which consists of an Application Load Balancer and an Auto Scaling Group of EC2 Instances running Linux and Apache HTTP servers. For its database tier, you also have a running RDS instance to host the MySQL database.
Which security measures fall within AWS responsibilities?

- Install the latest security patches on EC2 and RDS.

Explanation:-This option is incorrect because the security patches for EC2 instances are the responsibility of the customer and patches for RDS need to be set and scheduled by the customer.

- Ensure all communication between EC2 and ELB is encrypted.

Explanation:-This option is incorrect because encrypting the traffic between EC2 and ELB is optional.

- ✅ Protect against network packet sniffing.

Explanation:-This option is the correct answer. Please see the below AWS shared responsibility model. This falls on the Networking responsibility of AWS. Packet sniffing usually relies on network interfaces that are on promiscuous mode to sniff all traffic even those not intended for the instance. AWS hypervisor will not deliver any traffic to an instance that is not addressed to it.

- Protect the EC2 instances against attacks by enforcing the principle of least privilege access.

Explanation:-This option is incorrect because as per above diagram, protecting the EC2 instances via security groups is the responsibility of the customer.

Q48) You are instructed to secure a RDS MySQL database instance which is being used by an Auto Scaling group of On-Demand EC2 instances in your VPC. You also have to make sure that the database traffic is encrypted to meet the security compliance requirements.
Which of the following should you do to ensure maximum security for the database and its connections? (Choose 3)

- Create a VPC security group for your EC2 instances and a separate VPC security group for your MySQL instance.

Explanation:-You cannot encrypt a database after creation, which makes Option incorrect. However, you can take a snapshot of the created database and encrypt a copy of the snapshot instead.
Additionally, encrypting data in-transit by using SSL is a best practice in AWS Security. You should also have different security groups for your EC2 instances and MySQL instance since they handle different kinds of network traffic and connections.

- ✅ Create an EC2 security group for the servers and a DB security group for the MySQL database. Configure to only allow inbound traffic from the EC2 security group to the DB security group.

Explanation:-This option is incorrect because DB security groups are for database instances not in a VPC, but in an EC2-Classic platform.

- ✅ Use SSL created by Amazon RDS to encrypt database traffic.

Explanation:-You cannot encrypt a database after creation, which makes Option incorrect. However, you can take a snapshot of the created database and encrypt a copy of the snapshot instead.
Additionally, encrypting data in-transit by using SSL is a best practice in AWS Security. You should also have different security groups for your EC2 instances and MySQL instance since they handle different kinds of network traffic and connections.

- Create a dummy database to confuse attackers.

Explanation:-This option is incorrect because creating another database as a dummy won't protect your data. You'll also be charged more if you do this.

- ✅ Create a snapshot of the running MySQL instance and start a new encrypted MySQL instance from the encrypted copy of the snapshot.

Explanation:-You cannot encrypt a database after creation, which makes this option as incorrect. However, you can take a snapshot of the created database and encrypt a copy of the snapshot instead.
Additionally, encrypting data in-transit by using SSL is a best practice in AWS Security. You should also have different security groups for your EC2 instances and MySQL instance since they handle different kinds of network traffic and connections.

- Stop your MySQL instance and select instance actions. From there, click Enable Encryption to allow encryption on the data stored in the database.

Explanation:-You cannot encrypt a database after creation, which makes this option as incorrect. However, you can take a snapshot of the created database and encrypt a copy of the snapshot instead.
Additionally, encrypting data in-transit by using SSL is a best practice in AWS Security. You should also have different security groups for your EC2 instances and MySQL instance since they handle different kinds of network traffic and connections.

Q49) A mobile development company has various AWS resources to support its various mobile products. To keep control of costs, they have requested for you to get the billing alerts for your AWS account once it reaches a certain limit.
Which of the following should you enable before you can receive billing alerts in AWS?

Request an AWS support partner to notify you on estimated charges

Explanation:-This option is incorrect because AWS can already provide you with the options to enable and configure billing alerts for your account.

Request AWS support to notify you on estimated charges.

Explanation:-This option is incorrect because AWS can already provide you with the options to enable and configure billing alerts for your account.

Enable billing alerts in CloudWatch Console.

Explanation:-This option is incorrect because you need to enable billing alerts on your Preferences page.

Enable billing alerts in Account Preferences of the AWS Console.

Explanation:-This option is the correct answer. Before you can create an alarm for your estimated charges, you must enable billing alerts on your Accounts Preferences page first, so that you can monitor your estimated AWS charges and create an alarm using billing metric data. After you enable billing alerts, you cannot disable data collection, but you can delete any billing alarms that you created.

Q50) You are working for an IT Consulting company that has three separate AWS accounts in different regions with one VPC on each account. You manager instructed you to connect the three VPCs to each other and reminded you that these VPCs have no overlapping IPv4 or IPv6 CIDR blocks.
Which of the following is the most cost-effective connectivity option for this scenario?

Set up a NAT gateway on each VPC to connect to the other VPCs.

Explanation:-This option is incorrect because a NAT Gateway is mainly used to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances.

Set up an AWS Direct Connect connection for all three VPCs.

Explanation:-This option is incorrect as a Direct Connect connection is not cost-effective and is more suitable when connecting your on-premises data center to your VPC.

Use a VPN connection to connect all 3 VPCs.

Explanation:-This option is incorrect as a VPN connection is not a suitable option to use to connect two or more VPCs. You have to use VPC Peering instead.

Set up a VPC peering connection between the 3 VPCs.

Explanation:-A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

Q51) Your company has a VPC with a primary IPv4 CIDR block of 10.0.0.0/24 and 4 secondary IPv4 CIDR blocks. All available IP addresses have already been used up and you want to increase the size of the VPC to be able to add more EC2 instances.
How can you add a new subnet to your VPC?

You have to delete the unused subnets in your VPC to be able to create a new subnet.

Explanation:-In AWS, you assign a single Classless Internet Domain Routing (CIDR) IP address range as the primary CIDR block when you create a VPC and can add up to four (4) secondary CIDR blocks after creation of the VPC. In this scenario, you already have 4 secondary CIDRs and all of the IP addresses are already allocated which means that you cannot create secondary CIDRs anmore. On the given options, you can only add a new subnet if you delete an unused subnets in your VPC. Hence, this option is the corre

Add another secondary IPv4 CIDR block to increase the size of the VPC.

Explanation:-This option is incorrect because you can only add up to four (4) secondary CIDR blocks after the creation of the VPC.

Modify the primary IPv4 CIDR block to 10.0.0.0/25.

Explanation:-This option is incorrect because you cannot modify the existing CIDR block. Take note that a CIDR block of 10.0.0.0/23 is smaller the the current one.

Modify the primary IPv4 CIDR block to 10.0.0.0/23.

Explanation:-This option is incorrect because although the 10.0.0.0/23 CIDR block is bigger than the current size, you still cannot modify the existing CIDR block.

Q52) Your manager assigned you the task of implementing a highly available and scalable cloud architecture in AWS for their new online remittance system. You set up an Application Load Balancer and launched an Auto Scaling group of Spot EC2 instances on their UAT VPC. The QA team conducted performance testing on the new system and found out a defect in the application server. You want to investigate the problem and make the necessary changes without invoking the scaling down processes, which is why you temporarily suspended the Terminate scaling process.
What will be its effect on the Auto Scaling group's Availability Zone rebalancing process (AZRebalance) during this period?

The Auto Scaling group will not try to balance any longer the number of EC2 instances in the group across the Availability Zones in the region.

Explanation:-This option is incorrect.

The AZRebalance scaling process will automatically be disabled.

Explanation:-This option is incorrect.

The AZRebalance neither launches new instances nor terminates existing instances.

Explanation:-This option is incorrect.

The Auto Scaling group can grow up to ten percent larger than its maximum size.

Explanation:-You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. This can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes.
Amazon EC2 Auto Scaling can suspend processes for Auto Scaling groups that repeatedly fail to launch instances. This is known as an administrative suspension, and most commonly applies to Auto Scaling

---

Q53) A multinational financial firm is planning to deploy and test their prototype batch processing system on a set of EC2 instances in AWS. The system will process sample financial data for 6 hours once a week in a span of 8 months.
Which of the following would be the most cost-effective instance purchasing option to use in hosting the system?

Scheduled Instances

Explanation:-This option is incorrect because the prototype batch processing system will just run for 8 months. Although Scheduled Instances are suitable for scenarios where a compute capacity is needed for a specified recurring schedule, it is only recommended for at least a one-year term. If you choose this option, then you will still have to pay the whole term even if you already stopped using the instances, which is not cost-effective.

Reserved Instances

Explanation:-This option is incorrect because although Reserved Instances cost less, it is mainly used for a term from one to three years. Since the system will just run for 8 months, this is not a cost-effetive option because if you choose this, you will still have to pay the remaining term even if you already terminated the instances.

On-Demand Instances

Explanation:-This option is incorrect because On-Demand Instances cost more than Reserved and Spot instances.

Spot Instances

Explanation:-Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. For example, Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks.

Q54) An electronics manufacturing company has recently decided to adopt a hybrid cloud infrastructure that will store their backup data from their on-premises data center to AWS. You are instructed to upload their archive with a total size of 70 TB to Amazon Glacier. Using the AWS CLI, you uploaded a file named tutorialsdojo.zip to Glacier and received a response shown below. However, you noticed that you cannot assign a custom key name, such as tutorialsdojo.zip, to the archives that you upload.

{ "archiveId": "kKB7ymWJVpPSwhGP6ycSOAekp9ZYe_--zM_mw6k76ZFGEIWQX-ybtRDvc2VkPSDtfKmQrj0IRQLSGsNuDp-AJVlu2ccmDSyDUmZwKbwbpAdGATGDiB3hHO0bjbGehXTcApVud_wyDw",
"checksum":
"969fb39823836d81f0cc028195fcdbcbbe76cdde932d4646fa7de5f21e18aa67",
"location":
"/0123456789012/vaults/myvault/archives/kKB7ymWJVpPSwhGP6ycSOAekp9ZYe_--zM_mw6k76ZFGEIWQX-ybtRDvc2VkPSDtfKmQrj0IRQLSGsNuDp-AJVlu2ccmDSyDUmZwKbwbpAdGATGDiB3hHO0bjbGehXTcApVud_wyDw"
}

Which of the following options can you do to ensure that you can have the same file in Glacier in the most cost-effective way? (Choose 2)

Use AWS Snowmobile to upload the archive files to Glacier.

Explanation:-This option is incorrect because AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. This service is not suitable for transferring just a few terabytes of data.

Use AWS Snowball Edge to upload the archive files to Glacier by using the S3 lifecycle policy.

Explanation:-This option is incorrect because you only need to migrate 70TB which can be stored using a standard Snowball device. This is a more cost-effective option than Snowball Edge device.

Upload the archive files in Amazon S3 Infrequent Access. Set up a lifecycle policy to move the archives to Glacier.

Explanation:-In Amazon Glacier, an archive is any object, such as a photo, video, or document, that you store in a vault. It is a base unit of storage in Amazon Glacier. Each archive has a unique ID and an optional description. When you upload an archive, Amazon Glacier returns a response that includes an archive ID. This archive ID is unique in the region in which the archive is stored.
In Amazon Glacier, you cannot assign a key name to the archives you upload. Except for the optional archive descripti

Use the AWS Console to upload the archive file directly to Amazon Glacier.

Explanation:-This option is incorrect because the result will still be the same even if you use the AWS Console.

Use AWS Snowball to upload the archive files to Glacier by using the S3 lifecycle policy.

Explanation:-In Amazon Glacier, an archive is any object, such as a photo, video, or document, that you store in a vault. It is a base unit of storage in Amazon Glacier. Each archive has a unique ID and an optional description. When you upload an archive, Amazon Glacier returns a response that includes an archive ID. This archive ID is unique in the region in which the archive is stored.
In Amazon Glacier, you cannot assign a key name to the archives you upload. Except for the optional archive descripti

Set up a DynamoDB table and create a mapping of all the archive filenames to each archive IDs in Glacier.

Explanation:-This option is incorrect because setting up a separate DynamoDB table to map the archive IDs is not cost-effective as you have to pay the running cost of maintaining your DynamoDB instance. You can just use Amazon S3 instead.

Q55) A leading insurance firm has a VPC in the US East (N. Virginia) region for their head office in New York and another VPC in the US West (N. California) for their regional office in California. There is a requirement to establish a low latency, high-bandwidth connection between their on-premises data center in Chicago and both of their VPCs in AWS.
As the SysOps Administrator of the firm, how could you implement this in a cost-effective manner?

Set up two separate VPC peering connections for the two VPCs and for the on-premises data center.

Explanation:-This option is incorrect because VPC Peering is used to connect 2 VPC's together and not to connect your on-premises data center.

Set up an AWS VPN managed connection between the VPC in US East (N. Virginia) region and the on-premises data center in Chicago.

Explanation:-This option is incorrect because a VPN Connection is a more suitable solution for low to modest bandwidth requirements and can tolerate the inherent variability in Internet-based connectivity.

Set up an AWS Direct Connect gateway with a virtual private gateway.

Explanation:-You can use an AWS Direct Connect gateway to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different regions. You associate a Direct Connect gateway with the virtual private gateway for the VPC, and then create a private virtual interface for your AWS Direct Connect connection to the Direct Connect gateway. You can attach multiple private virtual interfaces to your Direct Connect gateway. A Direct C

Establish a Direct Connect connection between the VPC in US East (N. Virginia) region to the on-premises data center in Chicago and then establish another Direct Connect connection between the VPC in US West (N. California) region to the on-premises data center.

Explanation:-This option is incorrect because establishing two separate Direct Connect connections is expensive and hence, not a cost-effective option. It is better to establish a Direct Connect gateway instead which just uses one Direct Connect connection to integrate the 2 VPCs and the on-premises data center.

Q56) You are working as a SysOps Administrator in a well-funded technology startup which uses a set of Reserved EC2 instances in their VPC. During a recent IT audit, it was discovered that the operating system hosted on the EC2 instances is missing critical security patches, which must be urgently resolved.
Which of the following services can help you accomplish this task?

AWS Config

Explanation:-This option is incorrect because AWS Config simply records and evaluates the configurations of your AWS resources and does not deploy OS patches to your EC2 instances.

AWS Trusted Advisor

Explanation:-This option is incorrect because AWS Trusted Advisor is simply an online resource that helps you reduce cost, increase performance, and improve security by optimizing your AWS environment. Unlike AWS Systems Manager, this service cannot be used to update or deploy patches to your EC2 instance.

AWS Inspector

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 in AWS. This service does not deploy OS patches like AWS Systems Manager.

AWS Systems Manager

Explanation:-AWS Systems Manager helps you select and deploy operating system and software patches automatically across large groups of Amazon EC2 or on-premises instances. Through patch baselines, you can set rules to auto-approve select categories of patches to be installed, such as operating system or high severity patches, and you can specify a list of patches that override these rules and are automatically approved or rejected. You can also schedule maintenance windows for your patches so that they are

---

Q57) An IT Operations staff has created a new VPC with a CIDR block of 10.0.0.0/16 which has one subnet that has the same CIDR block as with the VPC. The staff tried to create another subnet of CIDR 10.0.1.0/24 but is prompted with an error in the AWS Console.
How can the staff create the second subnet?

Increase the size of the existing CIDR block.

Explanation:-This option is incorrect because you cannot increase or decrease the size of an existing CIDR block.

The staff can modify the CIDR block of the first subnet to allow more IP space and then try to add the second subnet.

Explanation:-This option is incorrect because you cannot modify the CIDR block of your subnet in AWS.

Associate secondary IPv4 CIDR blocks with your VPC.

Explanation:-You can associate secondary IPv4 CIDR blocks with your VPC to increase its size. When you associate a CIDR block with your VPC, a route is automatically added to your VPC route tables to enable routing within the VPC (the destination is the CIDR block and the target is local). Hence, Option is correct.
Take note that the scenario says that the VPC has a CIDR block of 10.0.0.0/16 which has one subnet that has the same CIDR block as with the VPC (10.0.0.0/16). This means that all available IP

The staff should be able to add the second subnet when he tries again.

Explanation:-This option is incorrect because unless the staff associates a secondary IPv4 CIDR block with their VPC, he/she will still see the error message everytime he/she tries to add a secondary subnet.

Q58) The latest Google Chrome browser marks non-HTTPS sites as 'not secure' to help users identify non-secure sites. Since the corporate website of your company is not using HTTPS, your manager instructed you to configure an SSL listener to their Classic Load Balancer and EC2 instances.
When implementing SSL, which of the following statement is incorrect?

When you use TCP (layer 4) for both front-end and back-end connections, your load balancer forwards the request to the back-end instances with modified headers.

Explanation:-This option is incorrect because when you use TCP (layer 4) for both front-end and back-end connections, your load balancer forwards the request to the back-end instances WITHOUT modifying the headers.

When you use HTTP (layer 7) for both front-end and back-end connections, your load balancer parses the headers in the request and terminates the connection before sending the request to the back-end instances.

Explanation:-Before you start using Elastic Load Balancing, you must configure one or more listeners for your Classic Load Balancer. A listener is a process that checks for connection requests. It is configured with a protocol and a port for front-end (client to load balancer) connections, and a protocol and a port for back-end (load balancer to back-end instance) connections.
The HTTPS protocol uses the SSL protocol to establish secure connections over the HTTP layer. You can also use the SSL protocol

If the front-end connection uses HTTP or HTTPS, then your back-end connections can use either HTTP or HTTPS.

Explanation:-Before you start using Elastic Load Balancing, you must configure one or more listeners for your Classic Load Balancer. A listener is a process that checks for connection requests. It is configured with a protocol and a port for front-end (client to load balancer) connections, and a protocol and a port for back-end (load balancer to back-end instance) connections.
The HTTPS protocol uses the SSL protocol to establish secure connections over the HTTP layer. You can also use the SSL protocol

If the front-end connection uses TCP or SSL, then your back-end connections can use either TCP or SSL.

Explanation:-Before you start using Elastic Load Balancing, you must configure one or more listeners for your Classic Load Balancer. A listener is a process that checks for connection requests. It is configured with a protocol and a port for front-end (client to load balancer) connections, and a protocol and a port for back-end (load balancer to back-end instance) connections.
The HTTPS protocol uses the SSL protocol to establish secure connections over the HTTP layer. You can also use the SSL protocol

---

Q59) As a Systems Administrator, you were instructed by your technical lead to set up an event notification for all system alerts happening on your RDS instance, which should be sent to the IT Operations team's emails and mobile phones.
Which of the following services will help you achieve this requirement?

AWS SNS

Explanation:-You can use AWS SNS to send event notifications as required on this scenario. According to AWS Documentation, Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables fan out notifications to end users using mobile push, SMS, and email. Amazon SNS is simple and cost effective to send push notifications to mobile device users, email recipients and email to other distributed services.

AWS CloudWatch

Explanation:-This option is incorrect because this service is used for logging metrics and monitoring AWS resources. You will still need the SNS service to create topics for sending email and SMS.

AWS SES

Explanation:-This option is incorrect because SES (Simple Email Service) is used as an AWS hosted emailing service.

AWS CloudTrail

Explanation:-This option is incorrect because CloudTrail is used for API logging services and activities across your AWS infrastructure. The requirement is to send event notifications.

Q60) An aerospace engineering company is having some issues in expanding their on-premises storage capabilities. The cost of upgrading their storage servers is too high and they need to find a more cost-effective option. The CTO decided to adopt a hybrid cloud architecture using AWS to extend their storage for their applications. The new storage should be available as an iSCSI target, which should be accessed by the servers in your on-premises data center.
Which of the following options would you use to meet this requirement?

S3 storage

Explanation:-This option is incorrect because although S3 is used as a scalable object storage, you still have to go through AWS Storage Gateway to set up an iSCSI target.

API Gateway

Explanation:-This option is incorrect because the AWS API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. This is not used as a storage service.

EBS Volumes

Explanation:-This option is incorrect because an EBS Volume is mainly used as a storage for EC2 Instances which reside in your VPC and not for your on-premises network.

✅ Storage Gateway

Explanation:-AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure. You can use the service to store data in the AWS Cloud for scalable and cost-effective storage that helps maintain data security. AWS Storage Gateway offers file-based, volume-based, and tape-based storage solutions.

Q61) You are a SysOps Administrator for a leading telecommunications company which uses a large Reserved EC2 instance to host their online customer portal. The Operations team noticed that the instance's public IP address is always changing when the instance is stopped or terminated. You are instructed to implement a solution to mask the failure of an instance by rapidly remapping the address to another EC2 instance in your VPC. Also, the public IP address of the EC2 instance should not change anymore.
Which of the following should you do to satisfy the requirement?

Launch the EC2 instance in a Placement Group.

Explanation:-This option is incorrect because a Placement Group simply determines how instances are placed on underlying hardware.

Enable the Enhanced Networking feature in the EC2 instance.

Explanation:-This option is incorrect because the Enhanced Networking feature is mainly used to provide high-performance networking capabilities for EC2 instances on supported instance types.

Use the Elastic Network Interface to create a static public IP address.

Explanation:-This option is incorrect because the ENI is only used to create and attach additional network interfaces for the EC2 instance.

✅ Attach an Elastic IP address to the EC2 instance.

Explanation:-An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account.
With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. An Elastic IP address is a public IPv4 address, which is reachable from the internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to

---

Q62) Your manager instructed you to set up a file system accessible to individuals across your organization and establish permissions for each user and group at the file or directory level. The file system should provide storage to access and share common data sets across multiple EC2 instances.
Which of the following options would you use to meet this requirement?

AWS ECS

Explanation:-This option is incorrect because ECS is used to host Docker instances and not as a file system.

AWS EBS

Explanation:-This option is incorrect because EBS is a block storage service that can only be assigned to individual EC2 Instances at a time.

✅ AWS EFS

Explanation:-Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and 4.1 (NFSv4) protocol.

AWS S3

Explanation:-This option is incorrect because S3 is mainly used as a scalable object storage service.

Q63) You are working as a SysOps Administrator for a tech startup company. Your manager instructed you to develop a mobile application which sends and fetches data to a DynamoDB table. The app is using the DynamoDB SDK and root account access keys to connect to DynamoDB.
Which of the following is the best option to improve the security of this architecture?

Create an IAM user which will be used solely by the mobile app, with web identity federation that validates calls to DynamoDB using a well-known third party identity provider such as Login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) 2.0 compatible provider.

Explanation:-This option is incorrect.

✅ Provision an IAM role with web identity federation that validates calls to DynamoDB using a well-known third party identity provider such as Login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) 2.0 compatible provider.

Explanation:-Web identity federation – You can let users sign in using a well-known third party identity provider such as Login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) 2.0 compatible provider. You can exchange the credentials from that provider for temporary permissions to use resources in your AWS account. This is known as the web identity federation approach to temporary access.
When you use web identity federation for your mobile or web application, you don't need to create custom

You should create a separate IAM user for the mobile app and attach a policy that provides access to DynamoDB.

Explanation:-This option is incorrect.

You should provision an IAM role with EC2 and DynamoDB access. Attach the IAM role to an EC2 instance which will route all calls coming from the mobile app to the DynamoDB table.

Explanation:-This option is incorrect.

Q64) You are working for one of the world's largest banks as an IT Consultant where you have acquired a new EC2 spot instance at a maximum price of $0.03 per hour. Less than an hour after acquiring this, the spot price increased to $0.05 per hour. How much will you be charged for running your spot instance for that hour?

$0.05

Explanation:-This option is incorrect.

$0.03

Explanation:-This option is incorrect.

$0.00

Explanation:-Remember the following guidelines for spot instance pricing:
If your Spot instance is terminated or stopped by Amazon EC2 in the first instance hour, you will not be charged for that usage. However, if you terminate the instance yourself, you will be charged to the nearest second.
If the Spot instance is terminated or stopped by Amazon EC2 in any subsequent hour, you will be charged for your usage to the nearest second. If you are running on Windows and you terminate the instance yours

$0.08

Explanation:-This option is incorrect.