Answer Sheet

Q1) In the tech startup where you are working as a Network Architect, an application uses a RESTful API hosted in AWS, which uses Amazon API Gateway and AWS Lambda. You were required by your manager to trace and analyze user requests as they go through your Amazon API Gateway API's and eventually to the underlying services.
Which of these options is the most appropriate tool that will meet the requirement?

● CloudWatch

Explanation:-This option is incorrect because CloudWatch is a monitoring and management service. It does not have the capability to trace and analyze user requests as they travel through your Amazon API Gateway APIs.

● VPC Flow Logs

Explanation:-This option is incorrect because VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your entire VPC. Although it can capture some details about the incoming user requests, it is still better to use AWS X-Ray as it provides a better way to debug and analyze your microservices applications with request tracing so you can find the root cause of your issues and performance.

● CloudTrail

Explanation:-This option is incorrect because CloudTrail is primarily used for API logging of all of your AWS resources.

✓ AWS X-Ray

Explanation:-You can use AWS X-Ray to trace and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services. API Gateway supports AWS X-Ray tracing for all API Gateway endpoint types: regional, edge-optimized, and private. You can use AWS X-Ray with Amazon API Gateway in all regions where X-Ray is available.
X-Ray gives you an end-to-end view of an entire request, so you can analyze latencies in your APIs and their backend services. You can use an X-Ray service m

---

Q2) You are the AWS Systems Engineer of a top insurance firm which has a fleet of on-demand Linux EC2 instances in AWS. You are writing a custom script that requires the AMI ID, instance type, MAC address, and other metadata of your EC2 instance to be able to properly monitor your systems.
Which of these options is the correct base URL that you must use to list all instance metadata?

● http://127.0.0.1/latest/

Explanation:-This option is incorrect because it refers to the loopback Internet protocol (IP) address.

● http://254.169.169.254/latest/

Explanation:- This option is incorrect because the URLs are incorrect - the numbers are not in the correct order.

✓ http://169.254.169.254/latest/

Explanation:-http://169.254.169.254/latest/meta-data/ is the URL that you can use to retrieve the Instance Metadata of your EC2 instance, including the public-hostname, public-ipv4, public-keys, et cetera. This can be helpful when you're writing scripts to run from your instance as it enables you to access the local IP address of your instance from the instance metadata to manage a connection to an external application. Remember that you are not billed for HTTP requests used to retrieve instance metadata a

● http://169.169.254.254/latest/

Explanation:- This option is incorrect because the URLs are incorrect - the numbers are not in the correct order.

Q3) You are working as the Systems Administrator for a leading bank which has a web application that is heavily using the RDS instance for its database tier. You are required to monitor how the different processes or threads on a DB instance use the CPU such as the percentage of the CPU bandwidth and total memory consumed by each process.
Which of the following is the most suitable solution to properly monitor your database?

✓ Enable Enhanced Monitoring in RDS.

Explanation:-Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console, or consume the Enhanced Monitoring JSON output from CloudWatch Logs in a monitoring system of your choice. By default, Enhanced Monitoring metrics are stored in the CloudWatch Logs for 30 days. To modify the amount of time the metrics are stored in the CloudWatch Logs, change the retention for the RDSOSMetrics log group in the Clou

● Set up a monitoring system which uses Amazon CloudWatch to track the CPU Utilization of your database.

Explanation:-This option is incorrect because although you can use Amazon CloudWatch to monitor the CPU Utilization of your database instance, it does not provide the percentage of the CPU bandwidth and total memory consumed by each database process in your RDS instance. Take note that CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance while RDS Enhanced Monitoring gathers its metrics from an agent on the instance.

● View the CPU% and MEM% metrics which are readily available in the Amazon RDS console.

Explanation:-This option is incorrect because the CPU% and MEM% metrics are not readily available in the Amazon RDS console, which is contrary to what is being stated in this option.

● Write a shell script that collects and publishes custom metrics to CloudWatch which tracks the real-time CPU Utilization of the RDS instance.

Explanation:-This option is incorrect because although you can use Amazon CloudWatch Logs and CloudWatch dashboard to monitor the CPU Utilization of the database instance, using CloudWatch alone is still not enough to get the specific percentage of the CPU bandwidth and total memory consumed by each database processes. The data provided by CloudWatch is not as detailed as compared with the Enhanced Monitoring feature in RDS. Take note as well that you do not have direct access to the instances/servers of you

---

Q4) An e-commerce platform that sells various products online is hosted on an Auto Scaling group of On-Demand EBS-backed EC2 instances. You have been instructed to get the following monitoring metrics related to EC2 instances to properly monitor the system performance:
- The amount of bytes read and written to the EBS volume
- The amount of Disk storage left on the EBS volume
- CPU Utilization for the underlying EC2 Instances
- Network Throughput of the EC2 Instances
Which of the following would require a custom CloudWatch metric for monitoring purposes?

● Both the amount of bytes read and written to the volume and the amount of Disk storage left on the EBS volume

Explanation:- These options are incorrect because these are metrics already defined on CloudWatch and are enabled by default for EC2 instances.

● Both CPU Utilization for the EC2 Instances and Network Throughput into the EC2 Instances

Explanation:- These options are incorrect because these are metrics already defined on CloudWatch and are enabled by default for EC2 instances.

✓ The amount of Disk storage left on the EBS volume

Explanation:-This option is the correct answer. You need a custom metric for the amount of disk storage left on the volume because it is not defined as an Amazon EBS metrics data point on CloudWatch.

● The amount of bytes read and written to the EBS volume

Explanation:- These options are incorrect because these are metrics already defined on CloudWatch and are enabled by default for EC2 instances.

● Network Throughput of the EC2 Instances

Explanation:- These options are incorrect because these are metrics already defined on CloudWatch and are enabled by default for EC2 instances.

● CPU Utilization for the EC2 Instances

Explanation:- These options are incorrect because these are metrics already defined on CloudWatch and are enabled by default for EC2 instances.

Q5) You are serving static content from your S3 bucket and using CloudFront service to speed up content delivery to your users across the globe. For your next business cycle, you plan on improving these services to attract more customers and provide them a better user experience. Therefore, you will be needing more information regarding the activities that are occurring in your AWS resources to plan your next step. AWS CloudFront includes a variety of reports you can use to see usage and activity that is occurring in your CloudFront distributions.
How will you utilize these reports for this matter? (Choose 3)

✓ Use Viewers Reports to determine the locations of the viewers that access your content most frequently.

Explanation:-These options are correct because you are using the correct report for each purpose. Popular Objects Report can determine what objects are frequently being accessed, and get statistics on those objects. Usage Reports tells you the number of HTTP and HTTPS requests that CloudFront responds to from edge locations in selected regions. Viewers Reports can determine the locations of the viewers that access your content most frequently.

✓ Use Usage Reports to know the number of HTTP and HTTPS requests that CloudFront responds to from edge locations in selected regions

Explanation:-These options are correct because you are using the correct report for each purpose. Popular Objects Report can determine what objects are frequently being accessed, and get statistics on those objects. Usage Reports tells you the number of HTTP and HTTPS requests that CloudFront responds to from edge locations in selected regions. Viewers Reports can determine the locations of the viewers that access your content most frequently.

✓ Use Popular Objects Report to determine what objects are frequently being accessed, and get statistics on those objects

Explanation:-These options are correct because you are using the correct report for each purpose. Popular Objects Report can determine what objects are frequently being accessed, and get statistics on those objects. Usage Reports tells you the number of HTTP and HTTPS requests that CloudFront responds to from edge locations in selected regions. Viewers Reports can determine the locations of the viewers that access your content most frequently.

● Use Usage Reports to learn about the different types of browsers that your users frequently use to access your content.

Explanation:-These option are incorrect because you are using the wrong report for each purpose.
You use Top Referrers Reports to display a list of the 25 website domains that originated the most HTTP and HTTPS requests for objects that CloudFront is distributing for a specified distribution.
You use Cache Statistics Reports to get statistics on viewer requests grouped by HTTP status code.
You use Viewers Reports to learn about the different types of browsers that your users use most frequentl

● Use Top Referrers Reports to get statistics on viewer requests grouped by HTTP status code.

Explanation:-These option are incorrect because you are using the wrong report for each purpose.
You use Top Referrers Reports to display a list of the 25 website domains that originated the most HTTP and HTTPS requests for objects that CloudFront is distributing for a specified distribution.
You use Cache Statistics Reports to get statistics on viewer requests grouped by HTTP status code.
You use Viewers Reports to learn about the different types of browsers that your users use most frequentl

● Use Cache Statistics Reports to display a list of the 25 website domains that originated the most HTTP and HTTPS requests for objects that CloudFront is distributing for a specified distribution.

Explanation:-These option are incorrect because you are using the wrong report for each purpose.
You use Top Referrers Reports to display a list of the 25 website domains that originated the most HTTP and HTTPS requests for objects that CloudFront is distributing for a specified distribution.
You use Cache Statistics Reports to get statistics on viewer requests grouped by HTTP status code.
You use Viewers Reports to learn about the different types of browsers that your users use most frequentl

---

Q6) A money transfer mobile app is heavily using RESTful web services which is hosted in an Auto Scaling group of Spot EC2 instances across multiple Availability Zones and a Load Balancer. You are setting up the monitoring system and you know that the web services currently utilize a lot of memory in order to function properly.
In this scenario, which of the following metrics should be used to monitor the memory usage?

✓ Custom metric

Explanation:-Take note that there is no "Memory Utilization" metric available in CloudWatch for EC2. You have to setup a custom metric to set this up.
The Amazon CloudWatch Monitoring Scripts for Amazon Elastic Compute Cloud (Amazon EC2) Linux-based instances demonstrate how to produce and consume Amazon CloudWatch custom metrics. These sample Perl scripts comprise a fully functional example that reports memory, swap, and disk space utilization metrics for a Linux instance.

● DiskReadOps

Explanation:-This option is incorrect as the DiskReadOps metric only monitors the disk performance.

● CPU Utilization

Explanation:-This option is incorrect as this only covers the CPU usage of your instance and not the memory utilization.

● Memory Utilization

Explanation:-This option is incorrect since there is no "Memory Utilization" metric in CloudWatch. You should create a custom metric for this.

Q7) You've been tasked to monitor an ELB for one of your web applications and your teammate asked you where to find the information such as the client's IP address, latencies, request paths, and server responses.
Which of the following can you use to get the above information?

● VPC Flow Logs

Explanation:-This option is incorrect.

● CloudTrail Logs

Explanation:-This option is incorrect.

● CloudWatch Logs

Explanation:-This option is incorrect.
✓ ELB Access Logs
Explanation:-Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.
Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balanc

---

Q8) It is a requirement in your work that you produce regular reports and statistics on your EC2 resource consumption across different regions. In an upcoming meeting, you are asked to present these findings to your CTO and Data Analytics team. Aggregating these statistics would detail a lot of information on your resource consumption with ease.
What is the procedure for viewing aggregation statistics in CloudWatch?

✓ There is no way to view aggregate statistics in CloudWatch. CloudWatch cannot aggregate data across Regions.
Explanation:-You can aggregate the metrics for AWS resources across multiple resources. Amazon CloudWatch cannot aggregate data across Regions. Metrics are completely separate between Regions. Take note that you can monitor AWS resources in multiple Regions using a single CloudWatch dashboard, but you cannot aggregate the data across Regions.
● Create a Lambda function that collects metrics from your EC2 instances, computes your desired statistical output, and sends it to CloudWatch for viewing.
Explanation:-This option is incorrect.
● Enable detailed monitoring on your EC2 instances.
Explanation:-This option is incorrect.
● Use CloudWatch Metric Math to query metrics and apply mathematical operations on these metrics.
Explanation:-This option is incorrect.

Q9) You are working as a Network Administrator for a commercial bank where you are tasked to manually set up a VPN connection to allow communication between the instances from your AWS VPC to your on-premises data center.
Which of the following steps is not required to perform a VPN connection setup?

● Configure your route table to include the routes used by your VPN connection.
Explanation:-This option is incorrect.
● Create a Virtual Private Gateway.
Explanation:-This option is incorrect.
✓ Specify the private Autonomous System Number (ASN) for the Amazon side of the gateway.
Explanation:-Setting up a VPN connection to AWS requires you to have both Virtual Private Gateway and Customer Gateway available. 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.
The option gives the correct answer here because when you create
● Create a Customer Gateway.
Explanation:-This option is incorrect.

Q10) A Senior Systems Administrator has recently launched an Auto Scaling group of Spot EC2 instances with an Application Load Balancer. To properly monitor all of the web applications in your VPC, your manager wants to enable the Detailed Monitoring feature in CloudWatch for the Auto Scaling group.
Which of the following statements is true about this feature?

● Auto Scaling will send CloudWatch data metrics every five minutes with no additional charge.
Explanation:-This option is incorrct because basic monitoring sends data metrics every 5 minutes, but Detailed Monitoring sends data metrics every minute.
● Auto Scaling will send CloudWatch data metrics every minute with no additional charge.
Explanation:-This option is incorrect because there is an additional charge for Detailed Monitoring. The basic monitoring is the default and has no additional charge.
● CloudWatch Detailed Monitoring does not support Auto Scaling.
Explanation:-This option is incorrect because CloudWatch Detailed Monitoring supports Auto Scaling.
✓ Auto Scaling will send CloudWatch data metrics every minute with an additional charge.
Explanation:-CloudWatch Detailed Monitoring supports mostly all AWS services including Auto Scaling and sends data every minute. Once enabled, detailed monitoring incurs additional cost.

Q11)

You have a health and fitness tracker application which is hosted on a fleet of Spot EC2 Instances in a public subnet of your VPC. As part of security monitoring, the IT Operations team noticed that there are several requests coming from this specific IP address: 137.33.105.110 that originates from a country where you do not have any users. The IT Security department has advised that all subsequent traffic from this IP address should be blocked.

How can you achieve this requirement in this scenario?

● Add an Inbound Rule for the Security Group which will deny incoming traffic from 137.33.105.110/24
Explanation:-This option is incorrect because you can't define an Inbound deny rule for Security Groups. You can only add allow rules to your Security Groups, and after all those allow rules, there is an implicit deny all rule.
✓ Add an Inbound Rule for the NACL which will deny incoming traffic from 137.33.105.110/32
Explanation:-Since the request is to block an Inbound request from a specific IP address, it must be stopped at a subnet level. You will need to add a rule to the Network Access Control List. And for a particular IP, you need to use the /32 netmask for the CIDR notation.
● Add an Inbound Rule for the NACL which will deny incoming traffic from 137.33.105.110/0.
Explanation:-This option is incorrect because 137.33.105.110/0 does not have the correct netmask as you need to declare /32 to only ban the specific IP address and not the entire sub network.
● Add an Outbound Rule for the Security Group for the Spot EC2 Instances to ensure that no traffic goes to that IP.
Explanation:-This option is incorrect because the rule needs to be added at the subnet level. You can't explicitly block an IP address in a Security Group though you can allow incoming traffic from a certain IP address.

Q12) You have two On-Demand EC2 instances in your VPC which are launched in subnet Tango and subnet Delta respectively. You logged into the first instance and tried to ping the second instance but it has no response. What are the two possible causes for this issue? (Choose 2)

● There is no Internet Gateway attached to the VPC.
Explanation:-This option is incorrect because there is no requirement to allow the EC2 instances to connect to the Internet, hence, the use of Internet Gateway (IGW) is unnecessary and totally unrelated with the issue.
● The subnet Delta is private while subnet Tango is public which is why the two instances could not connect to each other.
Explanation:-This option is incorrect because it does not matter whether the subnet is public or private as long as they both reside in one VPC. Take note that a public subnet basically means that it has a route to the Internet Gateway and a private subnet does not. Hence, the subnet type (public/private) is not related to the issue.
● There is no IAM role provisioned to the first instance.
Explanation:-This option is incorrect because an IAM role is not required to allow communication between two EC2 instances.
✓ The NACL on subnet Delta does not allow outbound ICMP traffic.
Explanation:-To allow traffic on two EC2 instances located on different subnets, you should properly configure their respective Security Groups as well as the Network ACL. Hence,
AWS provides two features that you can use to increase security in your VPC: security groups and network ACLs. Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets.
● The subnet Tango has no target route to subnet Delta in the route table.
Explanation:-This option is incorrect because every subnet that you create is automatically associated with the main route table for the VPC. Hence, you don't need to define a route from subnet Tango to subnet Delta.
✓ The second instance's security group does not allow inbound ICMP traffic.
Explanation:-To allow traffic on two EC2 instances located on different subnets, you should properly configure their respective Security Groups as well as the Network ACL. Hence,
AWS provides two features that you can use to increase security in your VPC: security groups and network ACLs. Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets. In most cases, security groups c

Q13) Large amounts of transactions are going through your banking system into your EC2 instances, causing degradation on its overall performance. After monitoring the event, you found out that the root cause of the problem is the data transferring to your EBS volumes. This is caused by a high volume of transactions exceeding your bandwidth capacity. What would be a cost-effective solution to optimize EBS performance?

● Throttle the incoming traffic to enable your instances and EBS volumes to cope up with the volume of transactions.
Explanation:-An Amazon EBS–optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance.
This Option is incorrect since throttling your network might cause your transactions to pile up and affect your banking operations, which is counterproductive from what you are trying to solve.
Refer
● Increase the number of instances supporting your system.
Explanation:-An Amazon EBS–optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance.
This Option is incorrect because you should try running an instance that supports EBS optimization first, and verify if EBS optimization will be enough to meet your performance requirements.
Reference
● Increase the number of EBS volumes for your instances.
Explanation:-An Amazon EBS–optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance.
This Option is incorrect because you should try to enable EBS optimization first before increasing the number of ELB volumes you have, and verify if EBS optimization will be enough to meet your performance
✓ If the instance type of your instance does not support EBS optimization, change your instance type to one that supports it.
Explanation:-An Amazon EBS–optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance.
References: https://aws.amazon.com/blogs/compute/improving-application-performance-and-reducing-costs-with-amazon-ebs-optimized-instance-burst-capability/
https://docs.aws.amazon.com/AWSEC2/latest/Use

Q14) You are working as an IT Consultant for a RegTech startup that utilizes machine learning to improve their financial regulatory processes. They have a fleet of Spot EC2 instances with an Application Load Balancer to host their online customer portal. There is a requirement to produce a report that provides a list of IP addresses that are accessing their portal, including the API request logs that went through all of their AWS resources. Which of the following can help you achieve this requirement?

● AWS CloudTrail and AWS Config
Explanation:-In this scenario, you have to use VPC Flow Logs and CloudTrail to get the IP traffic that goes in to your VPC and also to log all API requests made to your AWS resources.
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs an
● AWS CloudWatch and AWS CloudTrail
Explanation:-In this scenario, you have to use VPC Flow Logs and CloudTrail to get the IP traffic that goes in to your VPC and also to log all API requests made to your AWS resources.
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs an
● AWS VPC Flow Logs and AWS CloudWatch Logs

Explanation:-In this scenario, you have to use VPC Flow Logs and CloudTrail to get the IP traffic that goes in to your VPC and also to log all API requests made to your AWS resources.
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs an

✓ AWS VPC Flow Logs and AWS CloudTrail

Explanation:-In this scenario, you have to use VPC Flow Logs and CloudTrail to get the IP traffic that goes in to your VPC and also to log all API requests made to your AWS resources.
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs an

---

Q15) A large business technology company heavily uses AWS to run its suite of cloud-based enterprise resource planning (ERP) applications across multiple business units. To save on costs, they are planning to run automated start/stop scripts that turn off EC2 instances in the development and UAT environments during non-business hours.
Which of the following is the most suitable service to use for this scenario?

● Instance user data

Explanation:-Resource or service-specific tags are often used to filter resources during infrastructure automation activities. Automation tags are used to opt in or opt out of automated tasks or to identify specific versions of resources to archive, update, or delete. For example, many customers run automated start/stop scripts that turn off development environments during non-business hours to reduce costs. In this scenario, Amazon Elastic Compute Cloud (Amazon EC2) instance tags are a simple way to identif

● CloudWatch Logs

Explanation:-Resource or service-specific tags are often used to filter resources during infrastructure automation activities. Automation tags are used to opt in or opt out of automated tasks or to identify specific versions of resources to archive, update, or delete. For example, many customers run automated start/stop scripts that turn off development environments during non-business hours to reduce costs. In this scenario, Amazon Elastic Compute Cloud (Amazon EC2) instance tags are a simple way to identif

● Instance metadata

Explanation:-Resource or service-specific tags are often used to filter resources during infrastructure automation activities. Automation tags are used to opt in or opt out of automated tasks or to identify specific versions of resources to archive, update, or delete. For example, many customers run automated start/stop scripts that turn off development environments during non-business hours to reduce costs. In this scenario, Amazon Elastic Compute Cloud (Amazon EC2) instance tags are a simple way to identif

✓ Tags

Explanation:-Resource or service-specific tags are often used to filter resources during infrastructure automation activities. Automation tags are used to opt in or opt out of automated tasks or to identify specific versions of resources to archive, update, or delete. For example, many customers run automated start/stop scripts that turn off development environments during non-business hours to reduce costs. In this scenario, Amazon Elastic Compute Cloud (Amazon EC2) instance tags are a simple way to identif

---

Q16) A NodeJS application uses an S3 bucket to store user-generated data. The bucket policy should always be monitored to secure the data of the users and verify that the files are not publicly accessible over the Internet. You are also tasked to automate the assessment of your resource configurations and resource changes to ensure continuous compliance and self-governance across your AWS infrastructure.
Which of the following is the best approach to satisfy this requirement?

● Configure the bucket policy of the S3 bucket using IAM to prevent any unauthorized access.

Explanation:-AWS Config enables continuous monitoring of your AWS resources, making it simple to assess, audit, and record resource configurations and changes. AWS Config does this through the use of rules that define the desired configuration state of your AWS resources. AWS Config provides a number of AWS managed rules that address a wide range of security concerns such as checking if you encrypted your Amazon Elastic Block Store (Amazon EBS) volumes, tagged your resources appropriately, and enabled multi-

● Enable MFA Delete and Versioning in the S3 bucket.

Explanation:-AWS Config enables continuous monitoring of your AWS resources, making it simple to assess, audit, and record resource configurations and changes. AWS Config does this through the use of rules that define the desired configuration state of your AWS resources. AWS Config provides a number of AWS managed rules that address a wide range of security concerns such as checking if you encrypted your Amazon Elastic Block Store (Amazon EBS) volumes, tagged your resources appropriately, and enabled multi-

✓ Use AWS Config.

Explanation:-AWS Config enables continuous monitoring of your AWS resources, making it simple to assess, audit, and record resource configurations and changes. AWS Config does this through the use of rules that define the desired configuration state of your AWS resources. AWS Config provides a number of AWS managed rules that address a wide range of security concerns such as checking if you encrypted your Amazon Elastic Block Store (Amazon EBS) volumes, tagged your resources appropriately, and enabled multi-

● Configure the bucket policy to deny all read and write actions from unauthorized users.

Explanation:-AWS Config enables continuous monitoring of your AWS resources, making it simple to assess, audit, and record resource configurations and changes. AWS Config does this through the use of rules that define the desired configuration state of your AWS resources. AWS Config provides a number of AWS managed rules that address a wide range of security concerns such as checking if you encrypted your Amazon Elastic Block Store (Amazon EBS) volumes, tagged your resources appropriately, and enabled multi-

---

Q17) You are working for a large technology company that owns several IT Consulting firms and has individual AWS accounts. As the SysOps Administrator, you are responsible for setting up their cloud architecture, ensuring that they are able to centrally manage policies and billing for their multiple AWS accounts.
Which of the following options would you implement to satisfy this requirement?

● Use a separate IAM policy on each account.

● Use Consolidated Billing.

✓ Use AWS Organizations to connect all of their AWS accounts.

Explanation:-AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes.
Using AWS Organizations, you can create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts. You can also use

● Set up an IAM group for each IT consulting firm.

Q18) You are managing a batch processing system which is hosted on a set of EC2 instances and a Classic Load balancer. The EC2 instances are deployed across three Availability Zones: us-east-2a, us-east-2b, and us-east-2c. You noticed that it is taking a long time to complete the batch because there are some EC2 instances in the us-east-2b AZ which are quite slow in processing the incoming requests.
Which of the following metrics can provide you the total number of requests (HTTP listener) or connections (TCP listener) that are still pending to be routed to a healthy instance?

● SpilloverCount
Explanation:-The SurgeQueueLength provides the total number of requests (HTTP listener) or connections (TCP listener) that are pending routing to a healthy instance. The maximum size of the queue is 1,024. Additional requests or connections are rejected when the queue is full.
Suppose that your load balancer has us-west-2a and us-west-2b enabled, and that instances in us-west-2a are experiencing high latency and are slow to respond to requests. As a result, the surge queue for the load balancer nodes in
● BackendConnectionErrors
Explanation:-The SurgeQueueLength provides the total number of requests (HTTP listener) or connections (TCP listener) that are pending routing to a healthy instance. The maximum size of the queue is 1,024. Additional requests or connections are rejected when the queue is full.
Suppose that your load balancer has us-west-2a and us-west-2b enabled, and that instances in us-west-2a are experiencing high latency and are slow to respond to requests. As a result, the surge queue for the load balancer nodes in
● RequestCount
Explanation:-The SurgeQueueLength provides the total number of requests (HTTP listener) or connections (TCP listener) that are pending routing to a healthy instance. The maximum size of the queue is 1,024. Additional requests or connections are rejected when the queue is full.
Suppose that your load balancer has us-west-2a and us-west-2b enabled, and that instances in us-west-2a are experiencing high latency and are slow to respond to requests. As a result, the surge queue for the load balancer nodes in
✓ SurgeQueueLength
Explanation:-The SurgeQueueLength provides the total number of requests (HTTP listener) or connections (TCP listener) that are pending routing to a healthy instance. The maximum size of the queue is 1,024. Additional requests or connections are rejected when the queue is full.
Suppose that your load balancer has us-west-2a and us-west-2b enabled, and that instances in us-west-2a are experiencing high latency and are slow to respond to requests. As a result, the surge queue for the load balancer nodes in

Q19) You are working as an IT Consultant for an energy company that is operating an oil manufacturing plant. To ensure the safety of their employees, they need to measure the temperature of their facility every 5 minutes using smart sensors. They want to send the custom data metrics of their application to CloudWatch to view the data graphs visually.
Which of the below statements is true regarding the scenario above?

● A custom data metric from smart sensors are not supported by CloudWatch.
Explanation:-This option is incorrect because AWS CloudWatch supports uploading custom metrics.
● You can directly go to the AWS Console and upload the data to CloudWatch.
Explanation:-This option is incorrect because you cannot upload custom metrics via the AWS Console.
● Using AWS Snowball, the customer can import the data to CloudWatch.
Explanation:-This option is incorrect because you don't use Snowball to import data to CloudWatch. You can use AWS CLI or API to upload the data metrics to CloudWatch.
✓ You can use AWS CLI or API to upload the data metrics to CloudWatch.
Explanation:-Although there is no option on the AWS console to upload custom metrics, you can do so by using the AWS CLI or the API. To publish a single data point using CloudWatch for a new or existing metric, use the put-metric-data command with one value and the time stamp. aws cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --value 2 --timestamp 2018-10-10-14T08:00:00.000Z

Q20) You are maintaining a popular real estate listing website which is hosted in AWS. It is hosted on 4 On-Demand EC2 instances with an Application Load Balancer in front that evenly distributes the incoming traffic, and a MySQL RDS instance. Due to the recent TV and social media advertisements, the average response time for the website visitors has significantly increased as well as the CPU Usage of the EC2 instances. Upon further checking, you noticed that the CPU Usage of the EC2 instances is hitting 90% at peak times while the CPU Usage for the database is at 20% with an average database operations of 3000.
As the SysOps Administrator of the company, which two options could improve response times? (Choose 2)

● Upgrade to a higher RDS Instance type.
Explanation:-This option is incorrect as you don't need to upgrade your RDS instance since its CPU usage is low and stable.
● Upgrade to a Multi-AZ RDS instance with Read Replicas.
Explanation:-This option is incorrect as you don't need to upgrade your RDS instance since its CPU usage is low and stable.
● Configure an Auto Scaling group for the EC2 instances based on a memory load threshold.
Explanation:-This option is incorrect as there is no available metric in CloudWatch that checks the memory load threshold of an instance. This is a custom metric that you have to set up.
● Provision the EC2 instance with a higher number of allowed open TCP connections.
Explanation:-This option is incorrect because increasing the number of open TCP connections for an instance does not significantly improve the network bandwidth. You have to upgrade your instance to a higher EC2 type.
✓ Configure an Auto Scaling group for the EC2 instances based on a CPU load threshold.
Explanation:-You can upgrade your EC2 instance to a higher type and configure an Auto Scaling group. You can set up a policy that uses the Amazon CloudWatch CPU Utilization metric to scale up or scale down the number of EC2 instances.
✓ Switch to a different EC2 instance type that has a greater CPU/memory ratio.
Explanation:-You can upgrade your EC2 instance to a higher type and configure an Auto Scaling group. You can set up a policy that uses the Amazon CloudWatch CPU Utilization metric to scale up or scale down the number of EC2 instances.

Q21) A company has an application that is hosted on a fleet of EC2 instances with an Application Load Balancer that evenly distributes the incoming traffic. There once was an incident where a Junior DevOps Engineer accidentally made changes in the ALB in production that brought the whole application down. These situations should not happen again and hence, you have to monitor any activity or changes made to your AWS resources.
Which of the following services does not help you capture the monitoring information about the ELB activity?

● ELB API calls with CloudTrail
Explanation:-This option is incorrect because CloudTrail allows you to log all API calls including those made via the ELB.
● CloudWatch metrics

Explanation:-This option is incorrect because ELB publishes data points to Amazon CloudWatch for the load balancers and its backend instances. CloudWatch enables one to receive statistics about those data points.

✓ ELB health checks

Explanation:-ELB health checks are used to determine whether the EC2 instances behind the ELB are healthy or not. But it does not help in capturing the monitoring information for the ELB itself.

● ELB Access logs

Explanation:-This option is incorrect because this enables you to capture detailed information about requests sent to your load balancer and store these logs to S3.

Q22) You are working for a medical technology company which has a number of resources hosted in AWS. An upcoming external IT audit will be conducted on your AWS resources to meet the strict security compliance requirements of the company. As the Systems Administrator, you have been tasked to provide log files for all activities carried out on the existing AWS resources including all AWS API calls made.
Which of the following AWS services would you use to fulfill this requirement?

✓ AWS CloudTrail

Explanation:-AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides an event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

● AWS Config

Explanation:-This option is incorrect because AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. This is used mainly for ensuring your AWS resources have the correct configuration according to your specified internal guidelines.

● AWS Trusted Advisor

Explanation:-This option is incorrect because AWS Trusted Advisor will only give you recommendations to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, and follow best practices for your AWS resources.

● AWS CloudWatch Logs

Explanation:- This option is incorrect. Although you use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances and other services, this will not provide you with all the activities recorded for each AWS resource.

Q23) An international IT Consulting company is planning on setting up multiple accounts in AWS to separate their various departments and projects teams. For security purposes, the IT Security department has a requirement to ensure that certain services and actions are not allowed across all the accounts.
How would you achieve this in the most effective way?

✓ Use AWS Organizations and Service Control Policies to control services on each account.

Explanation:-AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes. It allows you to create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts.

● Contact AWS and request for them to deny the services not allowed to be used across accounts.

Explanation:-This option is incorrect since AWS should not be responsible for denying usage of service in an account.

● Create a common IAM policy that can be applied across all accounts.

Explanation:-This option is incorrect because it is not possible to create a common IAM policy.

● Activate Consolidated Billing feature across the account to control the services on each account.

Explanation:-This option is incorrect since Consolidated Billing is just another feature under AWS Organization.

Q24) You are working as the Lead Systems Administrator in a well-funded startup where you are tasked to set up an On-Demand EC2 Instance and a DynamoDB. The instance will host an AI-based web application that stores results to a DynamoDB table. Due to your hectic work schedule, you decided to delegate this task to your fellow Systems Administrator so she can complete the task on your behalf.
Which of the following policy permissions are required to allow you to properly delegate the task and securely implement the given requirement? (Choose 2)

✓ An IAM permission policy that allows a user to pass a role.

Explanation:-If you want to grant a user the ability to pass any of an approved set of roles to the Amazon EC2 service upon launching an instance, you need to have these three elements:
An IAM permissions policy attached to the role that determines what the role can do. A trust policy for the role that allows the service to assume the role. An IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. A trust policy is defined for the role that allow

● An IAM permission policy that allows the EC2 Instance to pass a role.

Explanation:-This option is incorrect because it is the user that should pass the role, not the EC2 instance.

● An IAM permission policy that allows the user to assume a role.

Explanation:-This option is incorrect because you need a trust policy for assuming a role, and it is not the user that should assume a role.

● A trust policy that allows the EC2 Instance to pass a role.

Explanation:-This option is incorrect because to do this, you need an IAM permission policy which is not applicable for this situation.

● A trust policy that allows an IAM user to assume a role.

Explanation:-This option is is incorrect because you need a trust policy that the EC2 instance can assume a role and not an IAM User.

✓ A trust policy that allows the EC2 Instance to assume a role.

Explanation:-If you want to grant a user the ability to pass any of an approved set of roles to the Amazon EC2 service upon launching an instance, you need to have these three elements:
An IAM permissions policy attached to the role that determines what the role can do. A trust policy for the role that allows the service to assume the role. An IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. A trust policy is defined for the role that allow

---

Q25) You are working for a global technology company which has thousands of employees around the globe that are using Amazon VPC Cloud. As part of the company's security compliance, IT auditors have requested a Credential report which contains a list of AWS users that contains their current status, their access key usage, and if they are using Multi-Factor Authentication (MFA) or not.

How can you generate the report required by the auditors?

● Go to AWS EC2 dashboard and download the Credential report.
Explanation:-This option is incorrcect.
● You can contact an AWS partner to generate the Credential report.
Explanation:-This option is incorrect since the IAM section already provides the report for you.
✓ You can go to AWS IAM Console and download the Credential report.
Explanation:-This option is the correct answer as you can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get this credential report from the AWS Management Console, the AWS SDKs and Command Line Tools, or the IAM API.
● You can call up AWS support and have them generate the Credential report for you.
Explanation:-This option is incorrect since the IAM section already provides the report for you.

Q26) You have finally finished developing your website which is ready to be deployed in AWS and be made publicly available over the Internet. But before you do so, the website should support HTTPS since it will be delivering confidential information over the network. Your website is required to meet regulatory and compliance requirements for encryption of data in transit.
Which of the following services will enable you to provision SSL/TLS certificates for your website for encryption of sensitive data in transit and authentication purposes?

● Amazon Artifact
Explanation:-This is incorrect because Amazon Artifact is a self-service audit artifact retrieval portal that provides AWS customers on-demand access to AWS' compliance documentation and AWS agreements. You won't be able to provision SSL/TLS certificates on Amazon Artifact to secure data in-transit.
● Amazon Route 53
Explanation:-This option is incorrect because Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. You use Route 53 to perform three main functions in any combination: domain registration, DNS routing, and health checking. It does not provide certificates to encrypt your network, unlike Certificate Manager.
● AWS IAM
Explanation:-This option is incorrect because AWS IAM is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated and authorized to use resources. It does not help you provision SSL/TLS certificates for your website.
✓ AWS Certificate Manager
Explanation:-AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks.

Q27) You start up 3 On-Demand EC2 instances that have an ELB and a DynamoDB attached to run your online game, and you are initiating a beta test to weed out some bugs. You brought in 15 people for the beta testing, and tell everyone to first visit the login screen before starting. However some of them cannot connect to your game while others are having no problem connecting at all.
What should you do to determine the cause of the problem?

● Check CloudWatch metrics if your instances are being overloaded by the number of connections.
Explanation:-This option won't help out much since your setup should have been enough to accommodate the number of people beta testing your game, and this is clearly a network problem.
● SSH into each instance to check server logs manually.
Explanation:-This option is also incorrect because this is too tedious to do, and you are not utilizing the most out of your AWS services. In addition, the other group of testers were able to successfully connect to your application, which means that there's nothing wrong with your instance.
✓ Create VPC Flow Logs to check if traffic is reaching all of your instances in CloudWatch.
Explanation:-You can use VPC Flow Logs in checking if network traffic is reaching to all of your instances.
● Set your security groups to allow all incoming connections.
Explanation:-This option is incorrect because exposing your network is a security risk, allowing outside threats access to your instances.

Q28) You recently transferred your whole system into AWS and it is once again peak season for your travel website. You are in the middle of analyzing how you are going to manage the load using past statistical data, and you have tried estimating the number of services you need to run to handle the peak times. Currently, the cloud architecture consists of 4 EBS-backed EC2 instances attached to an ELB and configured with Auto Scaling. For the database tier, you provisioned an RDS instance with 2 read replicas. Three days later, you start receiving emails that your website is not loading properly for some customers.
Which EC2 metrics do you think will help you figure out the cause of your problem? (Choose 3)

✓ Network Packets Out
Explanation:-This option is correct because the Network Packets Out metric will let you see the amount of packets being sent on all network interfaces by your instance.
✓ Network In
Explanation:-This option is correct because the Network In metric will let you see the amount of bytes being received on all network interfaces by your instance.
● Disk Write Operations
Explanation:-This option is incorrect because the Disk Read and Write Operations metrics are only applicable for instance store-backed AMI instances. Take note that the scenario described EBS-backed instances and not instance store-backed instances.
● Disk Read Operations
Explanation:-This option is incorrect because the Disk Read and Write Operations metrics are only applicable for instance store-backed AMI instances. Take note that the scenario described EBS-backed instances and not instance store-backed instances.
✓ CPU Utilization
Explanation:-Amazon EC2 sends metrics to Amazon CloudWatch. You can use the AWS Management Console, the AWS CLI, or an API to list the metrics that Amazon EC2 sends to CloudWatch. By default, each data point covers the 5 minutes that follow the start time of activity for the instance. If you've enabled detailed monitoring, each data point covers the next minute of activity from the start time.
This option is correct because the CPU Utilization metric will help you determine if the instances are being ov
● Disk Write Bytes

Q29)

You only have a limited budget to spend for AWS services each month. If you overspend it, the following month's budget will be deducted to cover the additional expenses.

What should you do to keep your costs in check?

✓ Set up a billing alarm in AWS CloudWatch.
Explanation:-Billing alarms are a great way to notify you if your services will shoot over your set budget.
● Compute your expenses regularly using the AWS Simple Monthly Calculator to know how long you should keep your resources running.
Explanation:-AWS Simple Monthly Calculator is useful when planning which AWS resources to use and for how long. However, the computed amount will only be an estimate of what your monthly cost will be.
● Configure your AWS Billing to terminate all instances if they start charging beyond your allocated budget.
Explanation:-This option is something that you should not be considering, especially with a production environment running. Suddenly terminating your instances is very detrimental to your system. Also, there is no such feature in AWS Billing.
● All of these
Explanation:-This option is incorrect.

Q30) A crowdfunding company has hired you for consultation services. They have set up many crowdfunding projects on their website using Lambda, CloudFront, and S3, and they have asked you to evaluate them. They say they want to add new features, such as logging statistical data on how much their website is being accessed, how successful their crowdfunding projects are, and a way to check if people within their company are maliciously modifying website content.
Which of the following will you recommend to address these requests in a cost-effective way? (Choose 4)

✓ Enable S3 access logging with policies and user roles that limit certain users from modifying S3 bucket contents.
Explanation:-This option has control who can access your S3 bucket content by using policies and IAM roles. In this way, there is a finer line on who is accountable for what resource.
✓ Use CloudTrail to log all activity within the AWS account.
Explanation:-AWS CloudTrail records activities that occur in your AWS account and stores event history. It can be very useful for auditing changes made into your S3 buckets and S3 objects.
● Turn on versioning and multi-factor authentication in S3 to see if contents are really being modified unwarily.
Explanation:-This option is incorrect because turning on versioning and MFA won't tell you who modified the object. However, this is good for securing the content.
● Create a Lambda function that periodically checks what projects are being accessed and how many users are accessing the website.
Explanation:-This option is incorrect because doing this would be wasteful and costly since you don't need to periodically call the Lambda function to do such a service. AWS has other tools that serve the role better, such as AWS CloudWatch and CloudFront logging features.
✓ Use CloudFront monitoring and usage reporting features to analyze access data and viewer data.
Explanation:-CloudFront offers monitoring, reports, and access logs to track activity for your CloudFront distributions.
✓ Create an event that sends you a notification using Amazon SNS if a project has reached funding expectations.
Explanation:-AWS Lambda can trigger functions for you like sending a notification through Amazon SNS at a reasonable cost.

Q31) You are setting up a PostgreSQL database server that runs on a Reserved EC2 instance which will be used by the various internal applications within your VPC. To simplify the naming convention of the database server, you are planning to allocate a custom domain name for the database.
Which of the following should you do to complete this task?

● Set up a publicly hosted zone in Route 53. Create an A or AAAA record, such as db.tutorialsdojo.com, and specify the IP address of the database server.
Explanation:-This option is incorrect.
● Set up a publicly hosted zone in Route 53. Create a CNAME record, such as db.tutorialsdojo.com, and specify the IP address of the database server.
Explanation:-This option is incorrect.
✓ Set up a private hosted zone in Route 53. Create an A or AAAA record, such as db.tutorialsdojo.com, and specify the IP address of the database server.
Explanation:-A private hosted zone is a container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains within one or more VPCs that you create with the Amazon VPC service.
Here's how private hosted zones work:
You create a private hosted zone, such as example.com, and specify the VPCs that you want to associate with the hosted zone. You create records in the hosted zone that determine how Route 53 responds to DNS queries for your domain
● Set up a private hosted zone in Route 53. Create a CNAME record, such as db.tutorialsdojo.com, and specify the IP address of the database server.
Explanation:-This option is incorrect.

Q32) You have a Classic Load Balancer in your VPC that distributes traffic to 2 running EC2 instances in ap-southeast-1a AZ and 8 EC2 instances in ap-southeast-1b AZ. You noticed that half of the incoming traffic goes to ap-southeast-1a, which over-utilizes the 2 instances and under-utilizes the other 8 instances in the other AZ.
What is the most probable cause of this issue?

● The Classic Load Balancer listener is not set to port 80.
Explanation:-This option is incorrect.
● The security group of the EC2 instances does not allow HTTP traffic.
Explanation:-This option is incorrect.
✓ Cross-Zone Load Balancing is disabled.
Explanation:-Cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled Availability Zone, and improves your application's ability to handle the loss of one or more instances.
When you create a Classic Load Balancer, the default for cross-zone load balancing depends on how you create the load balancer. With the API or CLI, cross-zone load balancing is disabled by default. With the AWS Management Console, the option to enable cross-zone load balancing is selec
● The Classic Load Balancer listener is not set to port 22.
Explanation:-This option is incorrect.

Q33) A data analytics company is heavily using AWS and has two VPCs in their account: VPC-A (10.10.0.0/16) and VPC-B (20.20.0.0/16). As their Systems Administrator, you established a VPC peering connection between the two VPCs which has an ID of pcx-tutsd0j0.
Which of the following route entries need to be added to the route tables to ensure that traffic can flow across the VPCs? (Select all that applies)

● In VPC-B – Destination: 10.10.0.0/16 and Target: 20.20.0.0/16
Explanation:-This option is incorrect.
✅ In VPC-B – Destination: 10.10.0.0/16 and Target: pcx-tutsd0j0
Explanation:-The AWS Documentation gives an example on this scenario. Basically from the current VPC standpoint, you declare the remote VPC IP block as Destination and choose the VPC peering connection ID as the target. This option is correct from VPC-B's standpoint.
● In VPC-A – Destination: 20.20.0.0/16 and Target: 10.10.0.0/16
Explanation:-This option is incorrect.
● In VPC-A – Destination: 10.10.0.0/16 and Target: pcx-tutsd0j0
Explanation:-This option is incorrect.
✅ In VPC-A – Destination: 20.20.0.0/16 and Target: pcx-tutsd0j0
Explanation:-The AWS Documentation gives an example on this scenario. Please see the reference link for detailed explanation. Basically from the current VPC standpoint, you declare the remote VPC IP block as Destination and choose the VPC peering connection ID as the target. This option is correct from VPC-A's standpoint.
● In VPC-B – Destination: 20.20.0.0/16 and Target: pcx-tutsd0j0
Explanation:-This option is incorrect.

Q34) You have recently been assigned to migrate a legacy web application to AWS Cloud. You have already prepared all the networking and security components in your head, and now you have to design the web application to be scalable. It would be too costly to redesign the database schema to a NoSQL database, hence, it maintains a relational database structure. Company employees also frequently use the web application to access customer information.
What resources should you provision to set up a scalable web application?

● EC2 servers with an ELB in front deployed in multiple regions, and an RDS instance with Multi-AZ deployment.
Explanation:-The primary focus here is to develop a scalable web application in AWS. Having an ELB for your EC2 servers will allow you to distribute the load among them. Auto Scaling will scale the number of running instances based on the parameters you've set. For the RDS, since we'll be expecting a lot of read statements, having a read replica set up will help manage the load.
This Option is incorrect for the same reasons . It should include Auto Scaling to meet the scalability requirement.
Refe
● EC2 servers grouped into an auto scaling group with an ELB in front, and a DynamoDB instance.
Explanation:-The primary focus here is to develop a scalable web application in AWS. Having an ELB for your EC2 servers will allow you to distribute the load among them. Auto Scaling will scale the number of running instances based on the parameters you've set. For the RDS, since we'll be expecting a lot of read statements, having a read replica set up will help manage the load.
This Option is incorrect because DynamoDB cannot be used as a relational database.
References:
https://docs.aws.ama
✅ EC2 servers grouped into an auto scaling group with an ELB in front, and an RDS instance with a read replica.
Explanation:-The primary focus here is to develop a scalable web application in AWS. Having an ELB for your EC2 servers will allow you to distribute the load among them. Auto Scaling will scale the number of running instances based on the parameters you've set. For the RDS, since we'll be expecting a lot of read statements, having a read replica set up will help manage the load. References:
https://docs.aws.amazon.com/aws-technical-content/latest/cost-optimization-automating-elasticity/cost-optimizatio
● EC2 servers with an ELB in front deployed in multiple regions, and an RDS instance with a read replica.
Explanation:-The primary focus here is to develop a scalable web application in AWS. Having an ELB for your EC2 servers will allow you to distribute the load among them. Auto Scaling will scale the number of running instances based on the parameters you've set. For the RDS, since we'll be expecting a lot of read statements, having a read replica set up will help manage the load. This Option is incorrect because deployment in multiple regions is for the sake of high availability, which is not what the questio

---

Q35) You are working as an IT Consultant for a tech startup that plans to launch its data analytics application, and which uses a MongoDB database and an NGINX server. You are instructed to provision a service that provides more than 200,000 IOPS in 4kB random I/O reads for the database.
Which of the following options will meet this requirement?

● Cold HDD (sc1) Volumes
Explanation:-Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications compared with EBS-backed EC2 instances.
If you use a Linux AMI with kernel version 4.4 or later and use all the SSD-based instance store volumes available to your instance, you get the IOPS (in 4kB block size) performance of o
● Throughput Optimized HDD (st1) EBS Volumes
Explanation:-Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications compared with EBS-backed EC2 instances.
If you use a Linux AMI with kernel version 4.4 or later and use all the SSD-based instance store volumes available to your instance, you get the IOPS (in 4kB block size) performance of o
✅ Storage Optimized Instances
Explanation:-Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications compared with EBS-backed EC2 instances.
If you use a Linux AMI with kernel version 4.4 or later and use all the SSD-based instance store volumes available to your instance, you get the IOPS (in 4kB block size) performance of o
● Provisioned IOPS SSD (io1) EBS Volumes
Explanation:-Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications compared with EBS-backed EC2 instances.
If you use a Linux AMI with kernel version 4.4 or later and use all the SSD-based instance store volumes available to your instance, you get the IOPS

(in 4kB block size) performance of o

Q36) A data analytics firm has opened a new service center in Africa and they want it to be operational in a few days. The new service center decided to contact the Company HQ to request a list of running AWS resources and configurations being used in other service centers. You have prioritized creating a CloudFormation template that includes these initial resources and configurations that are crucial for their operations. You tell them that remaining templates of less important things will follow. Which among the choices will you send out first?

● CloudFormation design that includes EC2 servers, CloudWatch custom metrics, and SQS configurations.
Explanation:-Given that the company is a data analytics firm, they should first be provided with the necessary tools that would enable them to perform data analytics at some velocity, such as RedShift and EMR. This Option is not a priority because CloudWatch is for monitoring your resources and SQS is for queueing messages needed by your resources.
References:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-whatis-howdoesitwork.html
https://docs.aws.amazon.com/AWSCloudForm
✓ CloudFormation design that includes EC2 servers, Redshift, and EMR configurations.
Explanation:-Given that the company is a data analytics firm, they should first be provided with the necessary tools that would enable them to perform data analytics at some velocity, such as RedShift and EMR.
References:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-whatis-howdoesitwork.html
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-template-resource-type-ref.html
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/working-with-tem
● CloudFormation design that includes EC2 servers, EBS, CloudFront settings, and S3 configurations.
Explanation:-Given that the company is a data analytics firm, they should first be provided with the necessary tools that would enable them to perform data analytics at some velocity, such as RedShift and EMR.
This Option is not a priority because CloudFront is a CDN service which is used for high content delivery availability and performance. S3, meanwhile, is used for object storage. References:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-whatis-howdoesitwork.html
htt
● CloudFormation design that includes EC2 servers, EBS, Data Pipeline protocols and ElastiCache configurations.
Explanation:-Given that the company is a data analytics firm, they should first be provided with the necessary tools that would enable them to perform data analytics at some velocity, such as RedShift and EMR. This Option is not a priority because Data Pipeline is used to automate movement and transformation of data. There is nothing to move or transform at this point because the primary tools aren't set up yet. ElastiCache is built for fast data retrieval from high throughput and low latency in-memory data

Q37) Your company recently adopted a hybrid cloud architecture which requires them to migrate some of their on-premises web applications to AWS. You created a CloudFormation template which automatically provisions AWS resources such as EC2 instances, ELB, and RDS instances. After running the stack using the CLI, it successfully launched the EC2 instances and the ELB, but it failed to create a new RDS instance.
In this scenario, what will the CloudFormation service do by default?

● By default, there will be a Wait Condition that will pause the stack creation and prompt the user to acknowledge the failure.
● By default, the CloudFormation will roll back and delete the stack.
● By default, the CloudFormation will complete the stack creation since the EC2 and EBS resources were already launched.
✓ By default, the CloudFormation will roll back the stack.
Explanation:-The create-stack CloudFormation CLI command creates a stack as specified in the template. After the call completes successfully, the stack creation starts. You can check the status of the stack via the DescribeStacks API.
It has an --on-failure optional parameter which determines what action will be taken if stack creation fails. Its default value is ROLLBACK which means that the CloudFormation service will automatically rollback the stack in the event of failures. The value must be one of

Q38) You are working as a SysOps Administrator for a multinational investment bank which recently adopted a hybrid cloud architecture. To migrate their on-premises applications to AWS Cloud, you are preparing a couple of CloudFormation templates which will automatically provision the required resources needed.
Which sections are required when designing a template? (Select all that applies)

● Conditions section
● Parameters section
● Format Version section
● Outputs section
Explanation:-Templates include several major sections. The Resources section is the only required section. Some sections in a template can be in any order. However, as you build your template, it can be helpful to use the logical order shown in the following list because values in one section might refer to values from a previous section.
Format Version (optional) The AWS CloudFormation template version that the template conforms to. The template format version is not the same as the API or WSDL version
● Metadata section
✓ Resources section

Q39) You are working as a SysOps Administrator for a major insurance company. Your firm plans to migrate their online customer portal, which uses a relational database, from their on-premises infrastructure to AWS. You are required to do the migration in a cost-effective and manageable manner.
Which of the following services would you choose for hosting the database in AWS?

● Elastic MapReduce
Explanation:-Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.
This Option is incorrect because Elastic MapReduce is mainly used to easily run and scale Big Data frameworks and not for hosting a relational database.
Reference:

https://docs.aws.amazon.com

● Redshift

Explanation:-Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

This Option is incorrect because Redshift is mainly used for (Online Analytics Processing) applications and as a data warehouse.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGu

✓ RDS

Explanation:-Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

● DynamoDB

Explanation:-Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

This Option is incorrect because DynamoDB is mainly used to host a NoSQL database.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

Q40) A leading media company is utilizing a wide range of instance store-backed and EBS-backed EC2 instances in their VPC. There are a couple of instances which always goes from the pending state to the terminated state immediately after restarting it.
Which of the following is a possible cause of this problem? (Choose 4)

✓ The instance store-backed AMI that you used to launch the instance is missing a required part.

Explanation:-If your EC2 instance goes from the pending state to the terminated state immediately after restarting it, then it could be caused by one of the following reasons:

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).

Reference:

https://docs.aws.am

✓ The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.

Explanation:-If your EC2 instance goes from the pending state to the terminated state immediately after restarting it, then it could be caused by one of the following reasons:

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).

Reference:

https://docs.aws.am

✓ An EBS snapshot is corrupt.

Explanation:-If your EC2 instance goes from the pending state to the terminated state immediately after restarting it, then it could be caused by one of the following reasons:

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).

Reference:

https://docs.aws.am

✓ You've reached your EBS volume limit.

Explanation:-If your EC2 instance goes from the pending state to the terminated state immediately after restarting it, then it could be caused by one of the following reasons:

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).

Reference:

https://docs.aws.am

● AWS does not currently have enough available On-Demand capacity to service your request.

Explanation:-If your EC2 instance goes from the pending state to the terminated state immediately after restarting it, then it could be caused by one of the following reasons:

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).

This Option is incorrect because th

● You have reached the limit on the number of instances that you can launch in a region.

Explanation:-If your EC2 instance goes from the pending state to the terminated state immediately after restarting it, then it could be caused by one of the following reasons:

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). This Option is incorrect because this op

Q41) You are managing a global cryptocurrency exchange portal which uses a total of 20 EC2 instances evenly deployed across 4 regions (5 instances per region). An Application Load Balancer has also been set up on each region to distribute the incoming traffic to the EC2 instances.
How can you set up your portal to maintain site availability if one of the 4 regions was to lose network connectivity for an extended period of time?

✓ 1. Set up a Route 53 Latency Based Routing Record Set that resolves to the Application Load Balancers in each region.2. Set the Evaluate

Target Health flag to true.
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 (tutorialsdojo.com or apex.tutorialsdojo.com), it determines which AWS Regions you've created latency records for, determines which region gives the use

● 1. Set up a Route 53 Latency Based Routing Record Set that resolves to an Application Load Balancer in each region. 2. Set an appropriate health check on each ELB.
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 (tutorialsdojo.com or apex.tutorialsdojo.com), it determines which AWS Regions you've created latency records for, determines which region gives the use

● 1. Set up a VPN Connection on each of the EC2 instances in each region. 2. Configure a failover using BGP in the case of a region-wide connectivity outage.
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 (tutorialsdojo.com or apex.tutorialsdojo.com), it determines which AWS Regions you've created latency records for, determines which region gives the use

● 1. Launch another Application Load Balancer to place in front of the EC2 instances across all regions. 2. Set an appropriate health check on each ELB.
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 (tutorialsdojo.com or apex.tutorialsdojo.com), it determines which AWS Regions you've created latency records for, determines which region gives the use

---

Q42) Tony is your company's new Junior SysOps Engineer. You are to give him a basic guide on Route 53 health checking. If more than 18% of health checkers report that an endpoint is healthy, Route 53 considers it healthy.
When configuring Route 53 HTTP/HTTPS health checks to your resources, what HTTP status code(s) should be returned for Route 53 to consider your resources healthy?

● 1XX, 2XX and 3XX
Explanation:-Your endpoints should respond with 2xx and 3xx response codes, which will tell Route 53 that your resources are healthy. Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html

● 1XX and 3XX
Explanation:-Your endpoints should respond with 2xx and 3xx response codes, which will tell Route 53 that your resources are healthy. Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html

✓ 2XX and 3XX
Explanation:-Your endpoints should respond with 2xx and 3xx response codes, which will tell Route 53 that your resources are healthy. Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html

● 1XX and 2XX
Explanation:-Your endpoints should respond with 2xx and 3xx response codes, which will tell Route 53 that your resources are healthy. Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html

---

Q43) You are running six EC2 instances deployed in three regions, which are strategically selected based on your customers' behavioral patterns. Suddenly, one of the regions experienced a power outage due to a storm, thus affecting your business. How would you maintain site availability in case an event like this occurs again in the future?
Assume that a short recovery downtime period is allowed.

● Configure auto scaling and ELB with health checks to every region where you have your instances running.
Explanation:-DNS active-active failover allows access to your unhealthy instances to be redirected to active instances. Together with latency based routing, customers accessing your web servers will be balanced throughout available healthy instances based on latency. Active-passive failover using failover-based routing is acceptable, however, you need to have a secondary group of healthy resources on standby. When your primary group of instances starts failing, only then will the second group be included. Si

● Configure a DNS active-active failover using geolocation based routing policy that resolves to an ELB, with Evaluate Target Health set to True.
Explanation:-DNS active-active failover allows access to your unhealthy instances to be redirected to active instances. Together with latency based routing, customers accessing your web servers will be balanced throughout available healthy instances based on latency. Active-passive failover using failover-based routing is acceptable, however, you need to have a secondary group of healthy resources on standby. When your primary group of instances starts failing, only then will the second group be included. Si

● Configure a DNS active-passive failover using failover based routing policy that resolves to an ELB, with Evaluate Target Health set to True.
Explanation:-DNS active-active failover allows access to your unhealthy instances to be redirected to active instances. Together with latency based routing, customers accessing your web servers will be balanced throughout available healthy instances based on latency. Active-passive failover using failover-based routing is acceptable, however, you need to have a secondary group of healthy resources on standby. When your primary group of instances starts failing, only then will the second group be included. Si

✓ Configure a DNS active-active failover using latency based routing policy that resolves to an ELB, with Evaluate Target Health set to True.
Explanation:-DNS active-active failover allows access to your unhealthy instances to be redirected to active instances. Together with latency based routing, customers accessing your web servers will be balanced throughout available healthy instances based on latency. Active-passive failover using failover-based routing is acceptable, however, you need to have a secondary group of healthy resources on standby. When your primary group of instances starts failing, only then will the second group be included. Si

---

Q44) You are creating a secure VPC for a web chat application and your manager wants to make sure that the backend is not accessible to the public. Web servers will be placed in a public subnet, while database servers will be placed in a private subnet. The database servers should still be able to fetch the critical software patches and updates from the public Internet. It is expected that many connections will be made by the web chat application so you have to allocate enough IP addresses available for use.
What are the steps in designing such a VPC?

✓ 1. Launch VPC Wizard and choose VPC with Public and Private Subnet including a NAT Gateway2. Allocate an IPv4 CIDR block of 10.0.0.0/163. Create a new Elastic IP address and attach it to your NAT gateway4. Set up the necessary security groups for the public and private subnets including a Network ACL for the NAT gateway

● 1. Launch VPC Wizard and choose VPC with Public and Private Subnet including a NAT Gateway2. Allocate an IPv6 CIDR block of 10.0.0.0/163. Create a new Elastic IP address and attach it to your NAT gateway4. Set up the necessary security groups for the public and private subnets including a Network ACL for the NAT gateway

Explanation:-For this type of VPC configuration, you first need to create an Elastic IP address for your NAT gateway, which will allow your private subnet to connect to the outside Internet. After launching the wizard, allocate an IPv4 CIDR block of value 10.0.0.0/16, which will supplement you with the IP range needed. Then attach your allocated elastic IP to finish creating your VPC and exit the wizard.
This option is incorrect because of various factors. First, you can only use egress-only Internet ga

● 1. Launch VPC Wizard and Choose VPC with Public and Private Subnet including an egress-only Internet gateway2. Allocate an IPv4 CIDR block of 10.0.0.0/16 3. Create a new Elastic IP address and attach it to your egress-only Internet gateway4. Set up the necessary security groups for the public and private subnets

Explanation:-For this type of VPC configuration, you first need to create an Elastic IP address for your NAT gateway, which will allow your private subnet to connect to the outside Internet. After launching the wizard, allocate an IPv4 CIDR block of value 10.0.0.0/16, which will supplement you with the IP range needed. Then attach your allocated elastic IP to finish creating your VPC and exit the wizard.
This Option is incorrect because, for IPv4, you cannot use egress-only Internet gateway.
Refere

● 1. Launch VPC Wizard and Choose VPC with Public and Private Subnet including a NAT Instance2. Allocate an IPv6 CIDR block of 10.0.0.0/163. Create a new Elastic IP address and attach it to your NAT Instance4. Set up the necessary security groups for the public and private subnets as well as for the NAT Instance (NATSG)

Explanation:-For this type of VPC configuration, you first need to create an Elastic IP address for your NAT gateway, which will allow your private subnet to connect to the outside Internet. After launching the wizard, allocate an IPv4 CIDR block of value 10.0.0.0/16, which will supplement you with the IP range needed. Then attach your allocated elastic IP to finish creating your VPC and exit the wizard.
This option is incorrect because of various factors. First, you can only use egress-only Internet ga

---

Q45) A school is planning on recreating their own website by adding new features to it and making it more interactive for visitors. Because of this, they would like to create subdomains that redirects to the new webpages, while reusing their old parent domain registered in an external DNS service for the main page of the website.
What would be a cost-effective solution for creating subdomains without having to migrate the parent domain?

● There is no way to do this in AWS.

Explanation:-AWS allows the creation of a subdomain that uses Route 53 as the DNS service without having to migrate the parent domain for a cheap cost. The steps for performing this can be found in the reference.
You don't need to register a new domain in Route 53 just for the purpose of creating the subdomains.
Reference:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingNewSubdomain.html

● Provision EC2 servers with elastic IPs attached to them, and use those to host the new webpages. Then use Route 53 A records to point to the elastic IPs, and create NS records to direct subdomain queries.

Explanation:-AWS allows the creation of a subdomain that uses Route 53 as the DNS service without having to migrate the parent domain for a cheap cost. The steps for performing this can be found in the reference.
You don't need to register a new domain in Route 53 just for the purpose of creating the subdomains.
This Option is too tedious to do. The school only needs a host for their subdomains. There are more efficient ways to solve the problem.
Reference:
https://docs.aws.amazon.com/Ro

● Create a new subdomain in Route 53 by registering a domain and transferring the server records to their current DNS service.

Explanation:-AWS allows the creation of a subdomain that uses Route 53 as the DNS service without having to migrate the parent domain for a cheap cost. The steps for performing this can be found in the reference.
You don't need to register a new domain in Route 53 just for the purpose of creating the subdomains.

Reference:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingNewSubdomain.html

✓ Create a Route 53 hosted zone for the subdomain. Add records for the new subdomain to your Route 53 hosted zone. Update the DNS service for the parent domain by adding name server records for the subdomain.

Explanation:-AWS allows the creation of a subdomain that uses Route 53 as the DNS service without having to migrate the parent domain for a cheap cost. The steps for performing this can be found in the reference.
You don't need to register a new domain in Route 53 just for the purpose of creating the subdomains.

Reference:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingNewSubdomain.html

---

Q46) The development team of a software company has just released the next version of their application in production. It is hosted in an Amazon ECS Cluster with RDS as its database and uses Route 53 as its DNS service. The new version of the application has undergone testing and now needs to be promoted to production from a separate environment. In order to have a smooth transition and avoid any unwanted outages, you need an initial set of traffic to be directed to the new version of the application for testing before doing the final cutover.
Which of the following will you implement on Route 53 to achieve this?

✓ 2 resource records based on Weighted Routing policy

Explanation:-Route 53 weighted routing policy lets you direct traffic to multiple resources in proportions that you specify. It lets you associate multiple resources with a single domain name or a subdomain and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software.
.
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

● 1 resource record based on Geolocation Routing policy

Explanation:-Route 53 weighted routing policy lets you direct traffic to multiple resources in proportions that you specify. It lets you associate multiple resources with a single domain name or a subdomain and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software.
This Option is incorrect since geolocation routing is used if you want to route traffic to a specific region based on the location of y

● 1 resource record based on Latency Routing policy

Explanation:-Route 53 weighted routing policy lets you direct traffic to multiple resources in proportions that you specify. It lets you associate multiple resources with a single domain name or a subdomain and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software.

This Option is incorrect since latency routing is used for resources in multiple AWS regions and you want to route traffic to the regio

● 2 resource records based on Simple Routing policy

Explanation:-Route 53 weighted routing policy lets you direct traffic to multiple resources in proportions that you specify. It lets you associate multiple resources with a single domain name or a subdomain and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software.

This Option is incorrect since simple routing policy is used to configure standard DNS records. If you specify multiple values on a sim

---

Q47) Your manager instructed you to set up the disaster and recovery plan of your cloud architecture in AWS. The requirement is to establish durable backup and archiving strategy for the company-owned financial documents, which should be accessible immediately for 6 months. It is expected that there would be a compliance audit every 3 years so you have to ensure that the files are still available on that period.
Which service should you use to fulfill these requirements in the most cost-effective manner?

✓ Upload data to an S3 bucket. Use lifecycle policies to move the data to Amazon Glacier for archiving.

Explanation:-You can use lifecycle policies to define actions you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time).

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another Amazon S3 storage class. For example:

When you know objects are infrequently accessed, you might transition them to the STANDARD_IA storage class. You might want to

● Upload the data on an encrypted EBS volume. Use lifecycle policies to move EBS snapshots into an S3 bucket and later into Glacier for archiving.

Explanation:-You can use lifecycle policies to define actions you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time).

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another Amazon S3 storage class. For example:

When you know objects are infrequently accessed, you might transition them to the STANDARD_IA storage class. You might want to

● Set up a Direct Connect connection to upload data to an S3 bucket. For archiving purposes, use IAM policies to move the data into Amazon Glacier.

Explanation:-You can use lifecycle policies to define actions you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time).

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another Amazon S3 storage class. For example:

When you know objects are infrequently accessed, you might transition them to the STANDARD_IA storage class. You might want to

● Set up a Storage Gateway to store data to an S3 bucket. Configure lifecycle policies to move the data to Redshift for archiving.

Explanation:-You can use lifecycle policies to define actions you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time).

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another Amazon S3 storage class. For example:

When you know objects are infrequently accessed, you might transition them to the STANDARD_IA storage class. You might want to

---

Q48) A Database Engineer has been given the task of allocating the necessary storage to their newly provisioned EC2 servers on various AWS Regions. Each independent server is expected to handle business operations that have large database workloads for separate applications. They also need to allocate a secure and separate storage to keep the backup scripts and log files for each application.
What should be the most cost-effective storage types to provision in this case? (Choose 2)

✓ Use Amazon EBS - Cold HDD volumes for the file system.

Explanation:-EBS Provisioned IOPS provides high disk read/write performance, which is optimal for large database workloads. Cold HDD, on the other hand, is very cheap and is great for infrequently accessed data.

Although Amazon EFS is a great option for managing file systems, can scale very well and can be shared by multiple EC2 instances, it is more costly than an EBS alternative and hence, not cost-effective.

Throughput Optimized HDD is more focused on throughput rather than IOPS, which can affec

● Use Instance Store Volumes as the root volume.

Explanation:-EBS Provisioned IOPS provides high disk read/write performance, which is optimal for large database workloads. Cold HDD, on the other hand, is very cheap and is great for infrequently accessed data.

Although Amazon EFS is a great option for managing file systems, can scale very well and can be shared by multiple EC2 instances, it is more costly than an EBS alternative and hence, not cost-effective.

Throughput Optimized HDD is more focused on throughput rather than IOPS, which can affec

● Use Amazon ElastiCache for the file system.

Explanation:-EBS Provisioned IOPS provides high disk read/write performance, which is optimal for large database workloads. Cold HDD, on the other hand, is very cheap and is great for infrequently accessed data.

Although Amazon EFS is a great option for managing file systems, can scale very well and can be shared by multiple EC2 instances, it is more costly than an EBS alternative and hence, not cost-effective.

Throughput Optimized HDD is more focused on throughput rather than IOPS, which can affec

● Use Amazon EBS - Throughput Optimized HDD volumes as the root volume.

Explanation:-EBS Provisioned IOPS provides high disk read/write performance, which is optimal for large database workloads. Cold HDD, on the other hand, is very cheap and is great for infrequently accessed data.

Although Amazon EFS is a great option for managing file systems, can scale very well and can be shared by multiple EC2 instances, it is more costly than an EBS alternative and hence, not cost-effective.

Throughput Optimized HDD is more focused on throughput rather than IOPS, which can affec

● Use Amazon EFS for the file system.

Explanation:-EBS Provisioned IOPS provides high disk read/write performance, which is optimal for large database workloads. Cold HDD, on the other hand, is very cheap and is great for infrequently accessed data.

Although Amazon EFS is a great option for managing file systems, can scale very well and can be shared by multiple EC2 instances, it is more costly than an EBS alternative and hence, not cost-effective.

Throughput Optimized HDD is more focused on throughput rather than IOPS, which can affec

✓ Use Amazon EBS - Provisioned IOPS SSD volumes as the root volume.

Explanation:-EBS Provisioned IOPS provides high disk read/write performance, which is optimal for large database workloads. Cold HDD, on the other hand, is very cheap and is great for infrequently accessed data.

Although Amazon EFS is a great option for managing file systems, can scale very well and can be shared by multiple EC2 instances, it is more costly than an EBS alternative and hence, not cost-effective.

Throughput Optimized HDD is more focused on throughput rather than IOPS, which can affec

---

Q49) A legacy application hosted in AWS is using a Classic Load Balancer to evenly distribute the incoming traffic to multiple Reserved EC2 instances. Lately, the application is experiencing intermittent unavailability issues which seems to be caused by their application servers.
Which of the following metrics can you use to check for server errors sent from the registered instances?

✓ HTTPCode_Backend_5XX
Explanation:-Your load balancer sends metrics to Amazon CloudWatch for the HTTP response codes sent to clients, identifying the source of the errors as either the load balancer or the registered instances. You can use the metrics returned by CloudWatch for your load balancer to troubleshoot issues.
The following are response code metrics returned by CloudWatch for your load balancer:
-HTTPCode_ELB_4XX -HTTPCode_ELB_5XX -HTTPCode_Backend_2XX -HTTPCode_Backend_3XX -HTTPCode_Backend_4XX -HTTPCode_Back
● HTTPCode_Backend_4XX
Explanation:-Your load balancer sends metrics to Amazon CloudWatch for the HTTP response codes sent to clients, identifying the source of the errors as either the load balancer or the registered instances. You can use the metrics returned by CloudWatch for your load balancer to troubleshoot issues.
The following are response code metrics returned by CloudWatch for your load balancer:
-HTTPCode_ELB_4XX -HTTPCode_ELB_5XX -HTTPCode_Backend_2XX -HTTPCode_Backend_3XX -HTTPCode_Backend_4XX -HTTPCode_Back
● HTTPCode_Backend_3XX
Explanation:-Your load balancer sends metrics to Amazon CloudWatch for the HTTP response codes sent to clients, identifying the source of the errors as either the load balancer or the registered instances. You can use the metrics returned by CloudWatch for your load balancer to troubleshoot issues.
The following are response code metrics returned by CloudWatch for your load balancer:
-HTTPCode_ELB_4XX -HTTPCode_ELB_5XX -HTTPCode_Backend_2XX -HTTPCode_Backend_3XX -HTTPCode_Backend_4XX -HTTPCode_Back
● HTTPCode_Backend_2XX
Explanation:-Your load balancer sends metrics to Amazon CloudWatch for the HTTP response codes sent to clients, identifying the source of the errors as either the load balancer or the registered instances. You can use the metrics returned by CloudWatch for your load balancer to troubleshoot issues.
The following are response code metrics returned by CloudWatch for your load balancer:
-HTTPCode_ELB_4XX -HTTPCode_ELB_5XX -HTTPCode_Backend_2XX -HTTPCode_Backend_3XX -HTTPCode_Backend_4XX -HTTPCode_Back

---

Q50) You configured CloudWatch monitoring on an On-Demand, EBS-backed EC2 instance which is deployed on ap-southeast-1 region.
Which of the following metrics will always show a value of 0?

● NetworkIn
✓ DiskReadOps
Explanation:-DiskReadOps is the metric that counts the completed read operations from all instance store volumes available to the instance in a specified period of time. To calculate the average I/O operations per second (IOPS) for the period, divide the total operations in the period by the number of seconds in that period.
If there are no instance store volumes, either the value is 0 or the metric is not reported. Hence, the correct answer is This Option. The same behaviour also applies with DiskWrite
● NetworkOut
● CPUUtilization

Q51) You have several SysOps teams creating Linux EC2 clusters on AWS. As per company policy for security groups of any EC2 instance, the SSH port should not be open to the public and should be configured to listen to a custom port.
How can you implement a monitoring system that notifies you when an instance does not follow these rules?

● Run a third-party scanning tool on your EC2 instances and have it generate a report of non-compliant instances.
Explanation:-You can also be notified when AWS Config evaluates your custom or managed rules against your resources. This is helpful if you want to ensure that your resources are compliant to a custom rule you defined. You can also configure AWS Config to stream configuration changes and notifications to an Amazon SNS topic. For example, when a resource is updated, you can get a notification sent to your email, so that you can view the changes.
AWS Config sends notifications for the following events:

● • Use a CloudWatch custom metric to check if a security group SSH port is open to the public, and then send a notification for non-compliance.
Explanation:-You can also be notified when AWS Config evaluates your custom or managed rules against your resources. This is helpful if you want to ensure that your resources are compliant to a custom rule you defined. You can also configure AWS Config to stream configuration changes and notifications to an Amazon SNS topic. For example, when a resource is updated, you can get a notification sent to your email, so that you can view the changes.
AWS Config sends notifications for the following events: