3.An application has multiple EC2 instances within an Auto Scaling Group (ASG). The ASG also has a simple scaling policy to meet the demand for fluctuating traffic. The application is scaling up and down repeatedly within the timeframe of an hour. What configuration changes could be made to reduce the cost and the frequency of scaling?

Increase the Cooldown timer

The cooldown period helps to ensure that your Auto Scaling group doesn't launch or terminate additional instances before the previous scaling activity takes effect. Increasing the Cooldown timer would reduce the frequency of scaling.

Auto Scaling supports cooldown periods when using simple scaling policies, but not when using other scaling policies. So be mindful of the type of scaling policy. In this case, a Cooldown timer is applicable. simple scaling policies are not recommended by AWS but can still be created. Step scaling policies are the replacements of simple scaling policies.

By reducing the frequency of scale-up policies will result in savings because you aren't running EC2 addtional EC2 instance when their not needed.

Increase the alarm period that triggers the scale down policy

Simple scaling policies are triggered based on choosing a CloudWatch Alarm. By increasing the alarm period will reduce the frequency of the scaling.

11.A company has an application running in us-east-1a. In the case of Availability Zone failure, the company needs to recover the volume and launch another instance in another Availability Zone such as us-east-1b. The company is not concerned with downtime and trying to save costs by running in a single AZ. How can the company ensure that it can recover from such a failure?

Continuously create Snapshots

https://docs.aws.amazon.com/ebs/latest/userguide/ebs-snapshots.html

13A company has an application running on EC2 instance which needs to store multiple documents which are uploaded via users. User's frequently uploads changes to their documents but with the same name. The company wants to allows users to roll back to previous documents. Which storage solution would best meet their needs?

Amazon S3 is the perfect storage layer for storing documents and other types of objects. https://aws.amazon.com/s3/

14A company has a requirement that does not allow them to use DocumentDB and so they must provision an EC2 instance with MongoDB. Their current requirements are they need at most 10,000 IOPS Which storage solution would meet their needs?

EBS General Purpose SSD

Large databases such as MongoDB requirer a higher amount of IOPS. General Purpose has a maximum of 16,000 IOPS. When that limit is reached then they should use Provisioned IOPS SSD but for now, they can use General Purpose.

https://docs.aws.amazon.com/ebs/latest/userguide/ebs-volume-types.html

17.Which of the following should be referred to if you want to map Amazon Elastic Block Store to an Amazon EC2 instance for AWS CloudFormation resources?

Reference the logical IDs of both the block stores and the instance

The logical ID must be alphanumeric (A-Za-z0-9) and unique within the template. Use the logical name to reference the resource in other parts of the template. For example, if you want to map an Amazon Elastic Block Store volume to an Amazon EC2 instance, you reference the logical IDs to associate the block stores with the instance.

You must create the JSON with all of the essential attributes as part of the CloudFormation template. In the resource section, you must refer to the logical IDs of both the block stores and the instances and configure them according to your needs.

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/resources-section-structure.html

18.A company wants to back up their on-premise storage volumes to AWS. What solution would meet their needs?

Use Storage Volume Gateway

Storage Gateway Volume gateway is for backing up your off-cloud storage volumes on S3.

22A company has an application running on an EC2 instance behind an Elastic Load Balancer. Whenever a user signs up the product manager wants to receive an email. Which solution would meet their needs?

Use the AWS SDK to publish the event to an SNS topic. Have a subscription to the SNS topic to receive that email

AWS SDK can be used to publish an event to an SNS Topic. A Subscription can be made to an SNS topic so the product manager can receive an email.

This is the ideal solution over SES because SNS is a plain text email and since this is internal notifications we don't care on the aesthetic of the email. Additionally, we would also be able to easily add an SNS text message so we have more future flexibility of notification methods.

27.A web-application needs to frequently read per second data from S3 bucket using Standard Access. How can the S3 bucket be configured to maximize its read performance?

No changes are necessary

If you are in Standard Class there is nothing additional for you to do to improve the read performance on AWS.

Question 29

A company has thousands of applications which needs to deliver JSON logs to S3 so they can be analyzed in Athena. These files need to be archived, encrypted as well as converted to parquet format. Logs are being sent every minute and the company wants to be able to analyze them as soon as possible. What solution can be used to prepare the log files?

Use Kinesis Firehose

Kinesis Firehose has the ability to archive, encrypt as well as transform JSON to parquet. Kinesis Firehose allows you to choose from a limited option of consumers. One being S3 which is where we need these files to be.

EXPLANATION

Amazon Kinesis Data Firehose: <https://aws.amazon.com/kinesis/data-firehose/>

Question 31

A company needs to ensure its production application remains highly available and fault-tolerant. The application needs 6 instances running at any given time to stay operational and cannot afford downtime. The application operations in us-east-2 (Ohio) which only has 3 Availability Zones. How many EC2 instances do they need within each AZ to ensure the resiliency of their application in the case of single AZ failure?

Create an Auto Scaling Group configured to run in all AZs. Set Min Capacity Setting to 9

An ASG will automatically launch instances evenly across all AZs.

3 us-east-2a

3 us-east-2b

3 us-east-2c

The failure of a single AZ would result in 6 instances remaining. The ASG would launch more instances in the two remaining AZs but downtime would not occur.

6 Instances in us-east-2a, and 6 in us-east-2b.

The failure of a single AZ would result in 12 or 6 instances remaining

6 us-east-2a

6 us-east-2b

0 us-east-2c

Question 32

A company needs 8 m5.large EC2 instanced backed by Application Load Balancer running in us-east-1 region and can tolerate the loss of a single Availability Zone. What distribution of instances across Availability Zones will result in the lowest cost possible?

4 EC2 instances in Availability Zones a through c

There would be 12 instances in total Losing one AZ would result in 8 instances.

4 x us-east-1a

4 x us-east-1b

4 x us-east-1c

Allocating 4 instances in each of 3 AZs (a-c) strikes a balance between cost and resilience. This setup provides sufficient redundancy to handle the failure of one AZ without incurring excessive costs associated with using more AZs than necessary. It meets the requirement of tolerating the loss of one AZ effectively and is likely the most cost-efficient option among those provided.

Question 33

Which of the following are caching solutions on AWS?

EC2

EC2 instances could be used to setup up open-source caching instance with an instance Type with high amount of memory. EC2 any kind of computing so you can do anything you like as long as you're willing to maintain the instances yourself.

CloudFront

SELECTED

CloudFront is CDN which caches static content at edge locations around the world.

Question 34

A web application which consists of a single EC2 instance that has an Elastic IP (EIP) is accessed by employees from remote locations. How can the IP addreses from the inbound traffic be audited to determine if they are company approved IP addresses?

VPC Flow Logs

Turning on VPC Flow Logs within your VPC will capture inbound traffic from the internet into your VPC. Within these logs contains the IP address of the source of the incoming request. VPC Flow Logs can be stored in CloudWatch Logs or S3 where you can analyze them further.

Question 35

A serverless application is composed of multiple AWS Lambda functions that are invoked by API Gateway endpoints. A user needs to investigate the failure of specific AWS Lambdas. Which AWS service will give them visibility into the cause of the failures?

X-Ray

AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. X-Ray is useful for finding where a problem has occurred when a request is passed along multiple Lambdas but not necessarily what the problem has occurred.

In order to determine what, logging must be inserted into the code of the Lambda which will then be tracked via CloudWatch Logs.

CloudWatch Logs

SELECTED

Within the code for your Lambda functions, you can insert logging which will then be streamed to CloudWatch logs so you can determine what has occurred with your Lamda function.

Question 36

A web-application has around 100 background job requests per second. Another EC2 instance is set up to process the jobs. How can these applications be integrated together to meet the demand of requests without batching?

AWS SQS Standard

SQS Standard allows for a nearly unlimited amount of messages per second. There is no requirement that the requests be in order so SQS Standard is suitable

**EXPLANATION**

[Amazon SQS FIFO (First-In-First-Out) Queues](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html)

Question 41

Which IAM policy condition key should be used if you want to check whether the request was sent using SSL?

AWS: secure transport

AWS provides the following predefined keys for all AWS services that support IAM for access control: AWS: current time and AWS: secure transport.

To determine HTTP or HTTPS requests in a bucket policy, use a condition that checks for the key "aws:SecureTransport". When this key is true, then request is sent through HTTPS. To comply with the s3-bucket-ssl-requests-only rule, create a bucket policy that explicitly denies access when the request meets the condition "aws:SecureTransport": "false". This policy explicitly denies access to HTTP requests.

What S3 bucket policy should I use to comply with the AWS Config rule s3-bucket-ssl-requests-only?

Question 42

An application running on an EC2 instance has a scoreboard. The top ten scores rarely change but have high reads. The scores after the top change more frequently and are not as read as often. It is important that the time to read and write has a guarantee of speed. Which two AWS services would meet these performance requirements?

DynamoDB

SELECTED

DynamoDB allows you to set a guarantee of read and write capacity per second. This application is using a scoreboard which suggests the application is a game in nature. The scoreboard is likely simple in terms of data structure and is suited for DynamoDB

ElastiCache

ElastiCache is a caching solution. Since the top ten scores do not frequently change but have high reads. ElastiCache can be used to remove the burden of these reads from DyanmoDB

Question 43

A company has popular web-application behind an Auto Scaling Group that has seasonal traffic. In the summer traffic rapidly grows and each year the number of traffic doubles. The rate at which the traffic grows is not predictable. Summer is approaching and the company needs to implement a solution which will meet the performance demands. What configuration change to Auto Scaling Group will help them meet the demand?

Target tracking scaling policy

With Target Tracking you can monitor a metric such as Average CPU Utilization. It is going to look at the utilization across all the running EC2 instances and when CPU Utilization reaches that threshold it will spin up another instance.

**EXPLANATION**

[Scheduled Scaling for Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html)

[Target Tracking Scaling Policies for Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html)

[Aggregating Statistics Across Resources](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/GetSingleMetricAllDimensions.html)

Question 44

A Solutions Architect needs to design a storage solution to archive rarely accessed financial documents. In the case of an audit, files must be retrieved within 3-5 hours. Which Glacier retrieval option would be the most cost-effective and meet the time requirement?

Standard retrieval

Standard retrieval is $0.01 per GB and retrieval time completes within 3–5 hours

**EXPLANATION**

Amazon S3 Glacier FAQs: [https://aws.amazon.com/glacier/faqs/#dataretrievals](https://aws.amazon.com/glacier/faqs/" \l "dataretrievals)

Question 45

A company has sensitive documents that they need to hold onto for 7 years in case of a surprise audit, and it's essential they store them in a highly resilient storage solution. The company has chosen to use S3 Glacier due to its low cost and resiliency. However, since an on-site audit can occur at random, documents from S3 Glacier need to be retrieved within minutes. Which retrieval option would meet their needs?

Expedited retrieval

Expedited retrievals to access data in 1-–-5 minutes.

**EXPLANATION**

[Retrieving Glacier Archives](https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html)

Question 50

A website for internal company use is hosted on S3 Static Website Hosting and has a CloudFront distribution in front of it to only allow authenticated users to access the website. The S3 website URL endpoint provided by default for AWS is still accessible and users outside the company are able to access the website. How can access be forced only through CloudFront?

Update Bucket Policy to ensure public access is not granted

In order for the Bucket Policy to already be accessible to the internet, a bucket policy statement exists. When you create your OAI is creating a new statement in the Bucket Policy but will not remove the existing one. You need to ensure it is removed and only the statement that grants the OAI access remains.

Create an Origin Access Identity

Origin Access Identity (OAI) is a special CloudFront user to restrict access to content to an S3 bucket. The OAI is used in the Bucket Policy so the bucket allows that user to access the private files.

**EXPLANATION**

[Restricting Access to Amazon S3 Content by Using an Origin Access Identity](http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html)

Question 51

A company has a web application and they want to capture real-time clickstream data from user activities for subsequent analysis. Which AWS service is most suitable for collecting and streaming this data in real-time?

Kinesis Data Streams

Kinesis Data Streams is the correct answer. This AWS service is specifically designed to capture, store, and stream real-time data from sources like web applications. It allows you to continuously collect and process large amounts of fast-moving, distributed data streams. In the context of the question, where the company wants to capture real-time clickstream data from user activities, Kinesis Data Streams offers the necessary functionality to collect and stream this data for subsequent processing or analysis.

**EXPLANATION**

Amazon Kinesis Data Streams: <https://aws.amazon.com/kinesis/data-streams/>

Streaming Data: <https://aws.amazon.com/streaming-data/>

**Question 53**

**A business wants to migrate a three-tier web application to AWS. For licensing considerations, the company needs to be able to control where the instances are placed and have visibility into the underlying sockets and cores.**

**Which compute model should be used to accomplish this task?**

EC2 Dedicated Hosts

Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2 so that you get the flexibility and cost-effectiveness of using your own licenses, but with the resiliency, simplicity, and elasticity of AWS.

Dedicated Hosts allow you to use your existing per-socket, per-core, or per-VM software licenses, including Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, or other software licenses that are bound to VMs, sockets, or physical cores, subject to your license terms.

Amazon EC2 Dedicated Hosts

Question 55

A company has documents which it must frequently access that will remain highly available and after 30 days the files can be deleted. Which storage solution will meet those needs?

S3

S3 by default replicates yout data across at least 3 AZs making it highly available. Lifecycle policies can delete files after creation based on the amounts of days defined by the user.

**EXPLANATION**

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

Question 56

A Solution Architect must choose a storage solution that is suited for continuously processing a large amount of data, and that can write to disk with a throughput of 500 MiB per second. Which storage solution would meet these performance requirements?

EBS Throughput Optimized HDD

EBS Throughput Optimized HDD (Hard Disk Drive) is specifically designed for workloads that require consistent, high throughput performance. It is optimized for sequential read and write operations, making it ideal for scenarios where large amounts of data need to be processed continuously.

**EXPLANATION**

[Amazon EBS Volume Types](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html)

Question 58

A company has developed a product in the form of an application, which they've containerized. This product has been purchased by multiple customers who use it for data analysis. The containers are hosted on AWS Elastic Container Service (ECS) within a single cluster managed by the company. It's crucial to ensure that each customer's container is isolated from others to maintain virtual privacy. What is the best way to achieve this isolation in ECS?

Security Group between containers

This is correct. Security groups in AWS act as virtual firewalls that control both inbound and outbound network traffic at the instance level. In the context of ECS, you can assign security groups to task definitions or directly to ECS services. By configuring these security groups properly, you can enforce network isolation between containers. This ensures that containers serving different customers cannot access each other, thereby maintaining the necessary isolation and privacy.

Ideal for scenarios where containers need to be isolated at the network level to prevent cross-communication or data leaks between containers belonging to different customers.

Question 59

A company has a High-Performance Computing (HPC) application which requires lowest latency possible between multiple EC2 instances. Which EC2 Placement Group offers the best performance this type of application?

Cluster Placement

packs instances close together inside an AZ

low-latency network performance for tightly-coupled node-to-node communication

well suited for High Performance Computing (HPC) applications

Clusters cannot be multi-AZ

Question 60

An application requires access to files being generated from thousands of EC2 instances running within the same VPC. The application needs to easily read these generated files some which can be greater than 5 TB in size. What would be a convenient way to share the files across multiple EC2 instances as a common store?

Amazon EFS

EFS is a file system which allows you to mount to thousands of EC2 instances within the same VPC. EFS is used as common store so multiple EC instances. EFS can handle files up to 53 TB in size. Data would also remain in the VPC where with S3 it would need to leave the customer's VPC.

**EXPLANATION**

[Amazon Elastic File System (Amazon EFS)](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEFS.html)

Question 61

A company running a Redshift Cluster need to securely import data from petabytes worth of data from S3 to generate financial reports. Both S3 and Redshift are operating within the same region. Due to the sensitive nature of these reports, how can the S3 data be securely transported to Redshift?

Enable Amazon Redshift Enhanced VPC Routing.

Amazon Redshift Enhanced VPC Routing allows Redshift to utilize VPC components such as VPC Endpoints when turned on. To keep your connection secure you want to keep all traffic within the AWS network.

If Enhanced VPC Routing was turned off and there was no VPC Gateway Endpoint to S3 than traffic would leave outbound to the internet which is not secure.

Create a VPC Gateway Endpoint for S3

VPC Gateway Endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. Only two services are supported for Gateway Endpoints:

S3

DynamoDB

So you need to use VPC Gateway Endpoint.

Question 63

An application is running within a private subnet and needs an outbound connection to the internet to fetch package updates. Which solution will provide that instance with a connection to the Internet?

Launch a NAT Gateway in the public subnet and create a route in the route table for 0.0.0.0/0 for the NAT

Correct. A NAT (Network Address Translation) Gateway allows instances in a private subnet to connect to the internet or other AWS services but prevents the internet from initiating connections with those instances. The NAT Gateway is placed in a public subnet, and the route table for the private subnet is configured to direct outbound traffic (0.0.0.0/0) to the NAT Gateway. This setup ensures that the instances can access the internet for tasks such as fetching package updates while remaining secure from inbound internet traffic.

**EXPLANATION**

[Route Tables](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html)

Question 64

A company has a web-application running in a single region and to be cost-effective they are not running any standby servers in another region in case of region failure. But in the case of such a disaster, they want to inform users of the interruption of service instead of the web-application being unresponsive and not resolving. What solution could they implement?

Use Route53 to failover to a website hosted on S3 Static Website Hosting in another region.

You can failover to a website hosted on a S3. This would allow time for the company to provision a new web-application in another region and ensure users are aware of the downtime. Since hosting a website is very inexpensive if not free then this is an ideal solution for this company.

Question 65

A company has an on-premise Cassandra database with an existing large workload which they are migrating to AWS to an EC2 Which EBS Volume Type would be most the most performance their use case?

EBS Provisioned IOPS SSD

Large database such as Cassandra requires a high amount of reads and writes. So this database needs Provisioned IOPS

**EXPLANATION**

[Amazon EBS Volume Types](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html)