1. 1. Question

You would like to serve images only to users who are visiting from the United States. Which of the following is the correct method?

* + Restrict IP addresses with NAT instance
  + Use security groups
  + **Store image files in Amazon S3 and set bucket policy**
  + **Take advantage of Amazon CloudFront‘s geo-restricted delivery**
  + Use Amazon API Gateway

**Incorrect**

Amazon CloudFront is a CDN service that distributes content from global bases called “edge locations“.  
CloudFront has a geo-restriction (geo-blocking) feature that allows you to distribute or block content to users in specific regions.

1. 2. Question

You, the solutions architect, are trying to create a new AWS account within your organization. Immediately after creation, we plan to implement several measures to protect the security of the root user of the AWS account from threats such as account takeover. Which of the following is the correct course of action (choose two)?

* + **Enable multi-factor authentication (MFA) for root user**
  + Encrypt and store the root user‘s access key ID and secret access key locally
  + **Change root user password to complex one**
  + IP restrictions for root user
  + Remove admin rights from root user

**Incorrect**

Immediately after creating an AWS account, take security measures to protect the root account with all administrative privileges.  
Usually, changing the password to a complicated one or enabling multi-factor authentication (MFA) at login reduces the risk of account hijacking by impersonation.

1. 3. Question

Which of the following services is suitable for storing large amounts of streaming data in Amazon S3 or Amazon Redshift for analysis?

* + Amazon Kinesis Data Streams
  + **Amazon Kinesis Data Firehose**
  + Amazon Kinesis Data Analytics
  + Amazon SQS
  + Amazon SNS

**Correct**

Amazon Kinesis Data Firehose is a service that allows you to easily distribute and store stream data to Amazon services (S3, Redshift, Elasticsearch Service) without having to build your own applications.  
Option 1 is incorrect. Amazon Kinesis Data Streams can store streaming data in near real time, and the registered data can be processed by your own application built on services such as Amazon EMR and Lambda.  
Option 3 is incorrect. Amazon Kinesis Data Analytics is a service that runs SQL queries on streaming data for real-time analytics.  
Option 4 is incorrect. Amazon SQS is a managed message queue (MQ) service.  
Option 5 is incorrect. Amazon SNS is a message notification service provided by AWS.

1. 4. Question

Your company runs a web application that many customers use. You have been asked to ensure that the MySQL database on Amazon RDS that stores the data for this system does not become a bottleneck.  
Which of the following is an effective way to prevent the MySQL database from becoming a bottleneck (choose two)?

* + Put ELB‘s Classic Load Balancer in front of the web application tier
  + **Using Amazon RDS Read Replicas**
  + **Placing Amazon ElastiCache in front of a MySQL database on RDS**
  + Take advantage of the Multi-AZ feature of MySQL databases on Amazon RDS

**Incorrect**

An Amazon RDS read replica is a read-only copy of the same database as the master database. Read replicas can be used to expand read-intensive databases, increasing read throughput and improving performance (option 2).  
Amazon ElastiCache is a managed in-memory database. Since processing is performed in memory, the load on the database can be reduced by caching data (option 3).

1. 5. Question

Which of the following is a good way to increase the redundancy of your Amazon Redshift cluster?

* + Change to a more capable instance type
  + Configure cross-region snapshots
  + **Enable Multi-AZ**
  + **increase the number of nodes**

**Incorrect**

Increasing the number of nodes clusters multiple databases together for greater fault tolerance.  
Option 1 is incorrect. Changing to a higher-performance instance type improves processing performance, but does not increase redundancy.  
Option 2 is incorrect. Cross-region snapshots allow backups to another region, but do not provide any additional redundancy.  
Option 3 is incorrect. Multi-AZ cannot be configured with Amazon Redshift.

1. 6. Question

Your company recently launched a website to provide content for a global audience. For this website, You would like to use Amazon CloudFront with an EC2 instance connected as an origin to deliver static content to users at high speed.  
Which is the right solution for application high availability?

* + Using Lambda@Edge for Amazon CloudFront
  + **Enable Amazon S3 Transfer Acceleration for Amazon CloudFront**
  + **Configure another EC2 instance in another Availability Zone as part of your origin**
  + Configure another EC2 instance as part of the origin server cluster in the same Availability Zone

**Incorrect**

By setting multiple EC2 instances as origins for the origin group, it is possible to set failover within the origin group.  
Option 1 is incorrect. Lambda@Edge is a service that executes code from edge locations, but does not contribute to high availability of static content delivery originating from EC2 instances.  
Option 2 is incorrect. CloudFront cannot use the Transfer Acceleration function of S3.  
Option 4 is incorrect. Even if EC2 instances are placed in the same Availability Zone (AZ), if an Availability Zone failure occurs, access to the origin EC2 instance will not be possible, so it cannot be said to be a configuration that achieves high availability.

1. 7. Question

A company is running a national television campaign. The company expects the campaign to increase traffic from 5 requests per minute to more than 5,000 requests per minute. The system is an application running on Node.js. Which of the following is the appropriate service or method to reliably handle traffic spikes?

* + AWS Lambda
  + Amazon ElastiCache
  + Prepare enough EC2 instances to handle the expected load
  + **Create an Auto Scaling group and scale out your EC2 instances**

**Correct**

By setting up Auto Scaling to automatically scale out the EC2 instances, it is thought that it will be possible to respond to unexpected traffic spikes.  
Option 1 is incorrect. AWS Lambda is a serverless computing service running on containers. Lambda‘s containers cold start and may not be able to keep up with traffic spikes.  
Option 2 is incorrect. Amazon ElastiCache is an in-memory database service and cannot run Node.js applications.  
Option 3 is incorrect. When processing with EC2, even if you prepare a number of instances that can handle the expected load, processing may not be able to continue if the expected load is exceeded.

1. 8. Question

A company is currently developing a business application. The database that stores the data of this application is required to have the performance to withstand the frequent registration, update, and deletion of large amounts of business data.  
It also envisions joining multiple tables to retrieve data in order to generate reports from the stored data. In addition, there is a need for the ability to automatically expand database storage in preparation for future data growth.  
Which is the most suitable service that can meet these demands?

* + Amazon DynamoDB
  + Amazon Glacier
  + **Amazon Aurora**
  + Amazon Redshift
  + **Amazon S3**

**Incorrect**

Amazon Aurora is one of the database engines supported by Amazon RDS, a managed relational database service. It is suitable for databases in which data is frequently updated and deleted, and you can issue SQL to join multiple tables and retrieve the target data from the joined tables. In addition, since Aurora is a fully managed database service, it also has the ability to automatically expand storage according to the amount of data.  
Option 1 is incorrect. Amazon DynamoDB is a NoSQL database service that retrieves the value stored in the database by specifying the key ID. It is not possible to retrieve data using SQL like a general relational database.  
Option 2 is incorrect. Amazon S3 Glacier is a great object storage for storing long term archives.  
Option 4 is incorrect. Amazon Redshift has a column-oriented architecture and is a data warehouse service suitable for aggregation and analysis of large amounts of data.  
Option 5 is incorrect. Amazon S3 is a highly durable object storage service that can store large amounts of data.

1. 9. Question

A company collects real-time IoT data from factories and saves it to disk storage. The amount of data to be collected has increased and throughput is becoming a problem.  
As a solution architect, you are looking to improve throughput by moving to an in-memory database. Which of the following solutions has higher availability and potential for increased throughput?

* + Amazon RDS for PostgreSQL
  + Amazon Aurora
  + **Amazon ElastiCache for Redis**
  + Amazon ElastiCache for Memcached

**Correct**

Amazon ElastiCache can be used as an in-memory database. ElastiCache can utilize Memcached and Redis as engines, but Redis is typically used for high availability requirements. Redis can be applied to store IoT data as it can be used as a data store as well as being able to increase availability with a master/standby configuration.

1. 10. Question

A company runs its corporate applications on EC2 instances in a single region. A solution architect understands that the application should be able to be deployed in another region in case of a wide-area disaster.  
Which of the following methods should be combined to achieve this (choose two)?

* + **Detach EBS volume on EC2 instance and copy detached EBS volume to Amazon S3**
  + **Launch a new EC2 instance from an Amazon Machine Image in another region**
  + Launch a new EC2 instance in another region and copy the volume to EBS stored in Amazon S3
  + **Copy an Amazon Machine Image of an EC2 instance and specify a different region as the copy destination**
  + Copy an EBS volume from Amazon S3 and launch an EC2 instance in the destination region using the EBS volume

**Incorrect**

As a response to a wide-area disaster, an Amazon Machine Image (AMI) that stores application information is required to start an application on an EC2 instance in another region (option 2).  
In order to copy the AMI with saved information to another region, it is necessary to specify the destination region when copying the AMI (option 4).

1. 11. Question

There are companies that use EC2 instances and Amazon DynamoDB to develop applications and provide services to their users.  
At one point, several users of this application consulted us about data that should have been deleted being displayed. Which of the following is the appropriate action you should take?

* + Use Amazon DynamoDB global table
  + Using Amazon DynamoDB Streams
  + Select on-demand for capacity mode
  + **Enable Consistent Read setting**

**Correct**

Amazon DynamoDB is characterized by an eventual consistency model. This means that the written data is reflected correctly over time (consistency is guaranteed over time), but depending on the timing of data reading, the written data may not be reflected. will be Therefore, it cannot be used for applications that require access to consistent data.  
If you are leveraging DynamoDB and want access to consistent data, enable the Consistent Read setting. So option 4 is the correct answer.  
Option 1 is incorrect. Amazon DynamoDB global table is a function that maintains data consistency in database tables located in multiple regions.  
Option 2 is incorrect. Amazon DynamoDB Streams is a function that detects historical information on data changes (addition, update, deletion) made to DynamoDB tables as events and retains them for 24 hours.  
Option 3 is incorrect. DynamoDB‘s capacity mode on-demand is a mode in which you are billed for data reads and writes performed on database tables.

1. 12. Question

One company expects the number of users of its applications to grow fivefold in one year. This application is hosted in one region and uses a MySQL database on Amazon RDS, an Application Load Balancer, and EC2 to host a website and its microservices that host static and dynamic content.  
What design changes would you recommend to support the company‘s growth? (Choose 2)

* + **Move static files from EC2 to S3**
  + **Using Amazon Route 53 Geolocation Routing Policy**
  + Scale your environment based on real-time CloudTrail logs
  + Create a dedicated Elastic Load Balancing for each microservice
  + **Create RDS read replicas and modify applications to use these replicas**

**Incorrect**

You need to think about how to improve the performance of your application, which is expected to be accessed more often.  
EC2 has a fixed instance type and needs to be adjusted each time according to the access load. For this reason, it is thought that using S3 will be able to respond appropriately to an increase in access. Therefore you should move static files from EC2 to S3.  
Option 5 is also correct.  
Having an RDS read replica can increase read throughput and improve performance.  
Option 2 is incorrect. Since this application is only hosted in a single region, it would not benefit from using Amazon Route 53 geolocation routing.  
Option 3 is incorrect. Since AWS CloudTrail acquires logs of operations (API calls) used in AWS accounts, it is not possible to monitor application access loads.  
Option 4 is incorrect. The Elastic Load Balancer (ELB) has a function to automatically scale according to the communication traffic load, and the ELB itself has redundancy, so there is no need to prepare an ELB dedicated to microservices.

1. 13. Question

A certain web application has an ELB Classic Load Balancer in the public subnet, and a reverse proxy server that can perform content-based distribution under it. The web server that runs the application is located in a private subnet. At some point, you notice an increase in traffic to this reverse proxy, and you are asked for a fix. Which of the following would be both scalable and cost-effective (choose two)?

* + **Replace Reverse Proxy with Classic Load Balancer**
  + **Add Auto Scaling to your web server**
  + **Add Auto Scaling to Reverse Proxy**
  + Change the web server to burstable t2 instance type
  + Change Classic Load Balancer to Application Load Balancer

**Incorrect**

By adding Auto Scaling to the reverse proxy server and web server, it is possible to automatically scale out and scale in according to the load situation, so it is the most scalable and cost effective method.

1. 14. Question

An application consists of a development environment (DEV) and a production environment (PROD). The EC2 instances in the DEV environment run for 10 hours each day during business hours. On the other hand, the EC2 instances in the PROD environment are running 24/7.  
As a solution architect, you need to determine a compute instance purchasing strategy to minimize costs. Which of the following is the most cost effective?

* + **Use Spot Instances for DEV environments and On-Demand Instances for PROD environments**
  + Use On-Demand Instances for DEV environments and Spot Instances for PROD environments
  + **Use Scheduled Reserved Instances for DEV environments and Reserved Instances for PROD environments**
  + Use On-Demand Instances for DEV environments and Scheduled Reserved Instances for PROD environments

**Incorrect**

Scheduled Reserved Instances are considered useful because the DEV environment only needs to be up at certain times. Also, since the PROD environment runs 24 hours a day, Reserved Instances are considered valid.  
Option 1 is incorrect. The DEV environment is expected to run during business hours, so using Spot Instances is not appropriate.  
Option 2 is incorrect. The PROD environment runs 24 hours a day, so using Spot Instances is not appropriate.  
Option 4 is incorrect. Because the PROD environment runs 24 hours a day, Reserved Instances may be more cost-effective than Scheduled Reserved Instances.

1. 15. Question

Which of the following best describes Amazon DynamoDB Accelerator (DAX)? (Choose 2)

* + Performance is inferior to Amazon DynamoDB, but it is a cost-effective NoSQL database service
  + It is a service that reads semi-structured data stored in Amazon S3 to Amazon DynamoDB at regular intervals and can handle data in S3 without accessing S3.
  + **Amazon DynamoDB in-memory cache service**
  + **Achieving latency of several milliseconds even when processing millions of requests per second**
  + A function that allows you to set scaling rules for Amazon DynamoDB, a fully managed service.

**Incorrect**

Amazon DynamoDB Accelerator (DAX) is a highly available, fully managed in-memory cache for DynamoDB (option 3). Millions of requests per second can be processed with response times in milliseconds (option 4).  
With DAX, you can reduce the number of reads for data stored in DynamoDB, thereby improving read throughput.

1. 16. Question

Your company‘s system needs to migrate multiple applications to the AWS cloud within a month due to the expiration of hardware maintenance. Each application needs to transfer about 50TB of data, and after the migration is complete, you need a network connection with secure and stable throughput between your company and AWS.  
How will you prepare for the initial data migration and a stable network after the migration?

* + **Leverage AWS Direct Connect for initial data migration and ongoing networking**
  + Use Site to Site VPN for initial data migration and ongoing network
  + **Use AWS Snowball for initial data migration and AWS Direct Connect for ongoing networking**
  + Use AWS Snowball for initial data migration and Site to Site VPN for ongoing networking

**Incorrect**

AWS Snowball is very effective as a means of transferring large amounts of data to AWS at once. Even after migration, Direct Connect can be expected to maintain secure and stable throughput.  
Option 1 is incorrect. Due to the sheer volume of data across multiple applications, AWS Direct Connect may not be able to complete the first data migration in less than a month.  
Option 2 is incorrect. Similarly, with a Site to Site VPN, the initial data migration may not be completed within a month, and it may be difficult to maintain stable throughput after the migration.  
Option 4 is incorrect. It is considered difficult to maintain stable throughput with Site to Site VPN.

1. 17. Question

A company has a two-tier website system with web servers in public subnets and database servers in private subnets.  
In this system, only the web server is accessible from the internet, but the database server needs internet access for software updates.  
Which of the following services would meet the requirements of this system?

* + **Build NAT gateway in public subnet**
  + Setting up placement groups
  + Allocate an Elastic IP to the database server
  + Set communication traffic from the Internet to “permit“ in the network ACL of the private subnet

**Correct**

A NAT gateway has a NAT function for connecting to the Internet from a private subnet. By using this feature, you can meet your requirements.  
Option 2 is incorrect. A placement group is a logical grouping of EC2 instances within a single Availability Zone (AZ). EC2 instances placed within the same AZ can be grouped, which enables faster processing than communication between different AZs or between different regions, but does not meet the system requirements of the question.  
Option 3 is incorrect. Elastic IP is a service that provides a fixed global IP address. You cannot connect to the Internet simply by assigning a fixed public IP.  
Option 4 is incorrect. A network ACL that allows communication traffic from the Internet is an inbound rule and is not a requirement for connectivity from the database server to the outside Internet.

1. 18. Question

Your company has a web application that makes requests to an API service on the backend. API services run on ELB-registered EC2 instances.  
Most API service calls finish very quickly, but endpoint calls that create objects in external services take longer. This causes timeouts on the client side and increases overall system latency.  
Which should be done to minimize the impact of slow endpoints?

* + Resize EC2 instance and increase memory capacity
  + Use Amazon SQS to offload long-running requests to asynchronous processing by separate workers
  + **Increase ELB idle timeout to allow long-running requests to complete**
  + **Use Amazon ElastiCache (Redis) to cache responses from external services**

**Incorrect**

By caching responses from external services in Amazon ElastiCache in advance, calls to external services, which are bottlenecks, become unnecessary, and performance can be expected to improve.  
Option 1 is incorrect. By increasing the memory size of the EC2 instance, the processing performance of the EC2 instance can be expected to improve, but the bottleneck is considered to be the calling of external services, and the processing of the EC2 instance is not the bottleneck, so it is appropriate. Not.  
Option 2 is incorrect. Splitting workers for asynchronous processing with Amazon SQS is not appropriate, as calling external services is considered a bottleneck.  
Option 3 is incorrect. Increasing the Elastic Load Balancer (ELB) idle timeout does not reduce latency.

1. 19. Question

You, who are part of the security team, are looking to restrict access to certain services or actions in all company-owned AWS accounts. Every AWS account is made up of organizations in AWS Organizations.  
Permissions should be set in a single location and scalable. Which of the following is the correct way to meet these requirements?

* + Create ACLs to restrict access to services or actions
  + **Create a security group that allows the account and attach it to the user group**
  + Deny access to services or actions by creating cross-account roles in each account
  + **Create a service control policy at the root organizational unit to deny access to a service or action**

**Incorrect**

By using AWS Organizations service control policies, you can perform access control collectively for organizational units.  
Option 1 is incorrect. There is no function to restrict access for all AWS accounts using ACL.  
Option 2 is incorrect. Security groups are not a function for restricting access to AWS accounts.  
Option 3 is incorrect. Although access can be restricted by cross-account roles, this does not meet the requirements of the question as it must be set for each account.

1. 20. Question

As part of securing the API layer built on Amazon API Gateway, you need to authorize users who have been authenticated by your existing identity provider. If a user fails authentication three times, they should be denied access for one hour.  
Which of the following is the correct way to meet these requirements?

* + Add Minimum Permissions to IAM Roles Using IAM Authentication
  + **Invoke a Lambda function using Amazon API Gateway custom authentication to validate each user‘s identity**
  + Use Cognito User Pools and provide built-in user management
  + Use Cognito User Pools and integrate with external identity providers

**Correct**

You can work with Lambda in Amazon API Gateway custom authorization, so you can run programs that allow or deny access based on conditions.  
Option 1 is incorrect. IAM roles can be granted permissions in a whitelist format, but it is not possible to implement a mechanism that matches the requirements of the problem with IAM services alone.  
Options 3 and 4 are incorrect. Authentication using Cognito User Pools has the ability to lock user accounts, but it is not possible to implement a mechanism that matches the requirements in question.

1. 21. Question

You, a database administrator in the information systems department, received a request to migrate data to the AWS cloud. Upon investigation, you found that 50000 IOPS would be required per volume.  
Which is the right solution for storing data on EBS?

* + Select Throughput Optimized HDD (st1) for volume type
  + Select General Purpose SSD (gp2) for volume type
  + **Select Provisioned IOPS SSD (io1) as the volume type and create an EC2 instance of Nitro System to connect with this EBS**
  + Select Provisioned IOPS SSD (io1) as the volume type and create a non-Nitro System EC2 instance connected to this EBS

**Correct**

EBS has different performance characteristics depending on the volume type. Volume types with more than 50000 IOPS can only be io1 or io2 with Provisioned IOPS SSD. However, only if you choose the Nitro System, the maximum is 64000 IOPS. Even if you choose a Provisioned IOPS SSD, you‘ll still get up to 32000 IOPS on non-Nitro Systems.

1. 22. Question

A company is looking for a solution to store video archives of old news footage on AWS. It is rarely necessary to restore the video data, but when the data is needed it should be available within five minutes at the most, and costs should be kept to a minimum.  
Which of the following is the most cost-effective solution?

* + **Store your video archives in Amazon S3 Glacier and use the Expedited option**
  + Store your video archives on Amazon S3 Glacier and use the Standard option
  + **Store video archives in Amazon S3 Standard Infrequent Access**
  + Storing video archives in Amazon S3 with One Zone-Infrequent Access

**Incorrect**

By using Amazon S3 Glacier, you can keep costs lower than Amazon S3. The Expedited option allows data retrieval in 1-5 minutes.  
Option 2 is incorrect. Standard option requires 3-5 hours to retrieve data.  
Option 3 is incorrect. S3‘s standard infrequent access can keep costs down, but since the retrieval frequency is unknown, it is not possible to determine whether infrequent access is appropriate.  
Option 4 is incorrect. One-zone infrequent access can also keep costs down, but it also increases the chances of data loss because you are only storing data in a single zone.

1. 23. Question

Application A and application B with Auto Scaling are running on the same subnet. If you want to allow communication from application A to application B, but deny communication from application B to application A, which of the following is the correct setting (choose two)?

* + **Do not set inbound communication from the IP address of application B in the security group settings of application A.**
  + **Deny inbound communication from application B‘s IP address in application A‘s security group settings**
  + **Application B‘s security group settings allow outbound communication to IP addresses other than Application A‘s**
  + Network ACL set on the subnet to allow inbound communication from Application A‘s IP address
  + Deny inbound communication for Application B‘s IP address in the network ACL set on the subnet

**Incorrect**

Security group inbound communication is not allowed unless you explicitly specify an IP address. (option 1)  
Security group outbound communication can allow communication to specific IP addresses, so communication to unconfigured IP addresses will be denied (option 3)

1. 24. Question

A company‘s web application uses multiple Linux instances and stores data on EBS volumes. The company is looking for a solution that makes its applications more resilient in the event of a failure and provides atomicity, consistency, isolation and durability (ACID) compliant storage. Which of the following solutions best meets these requirements?

* + Launch your application on an EC2 instance in each Availability Zone (AZ) and attach an EBS volume to each EC2 instance
  + Configure an Auto Scaling group in multiple AZs and create an Application Load Balancer. Mount instance store on each EC2 instance
  + **Configure an Auto Scaling group in multiple AZs and create an Application Load Balancer. Store your data on Amazon EFS, each EC2 instance mount the target on the chest**
  + Configure an Auto Scaling group in multiple AZs and create an Application Load Balancer. Store data using Amazon S3 One Zone-Infrequent Access.

**Correct**

EFS is a highly available storage service that can be consumed by multiple EC2 instances. It is also considered a suitable storage because it has strong consistency.  
Option 1 is incorrect. Since EBS cannot be shared across Availability Zones (AZs), it must be replicated using clustering software, etc., but if a failure occurs, it will be difficult to comply with ACID.  
Option 2 is incorrect. Since the instance store is a volatile disk, data will be lost when the EC2 instance stops, making it unsuitable.  
Option 4 is incorrect. Amazon S3 uses an eventual data consistency model, so data consistency cannot be guaranteed.

1. 25. Question

A company runs web services on EC2 instances registered with an Application Load Balancer.  
EC2 instances run in Auto Scaling groups across two Availability Zones (AZs). This application requires a minimum of 4 EC2 instances to meet the required SLA. In the event of a single AZ failure, which of the following strategies would the company adopt to maintain its SLA at a lower cost?

* + Add a scaling policy with a short cooldown period
  + Change the Auto Scaling Group Launch Configuration to Use a Larger Instance Type
  + **Modify the Auto Scaling Group to use a total of 6 EC2 instances in 3 AZs**
  + **Modify the Auto Scaling Group to use a total of 8 EC2 instances in 2 AZs**

**Incorrect**

A total of 6 EC2 instances are running in 3 Availability Zones (AZ), so we can see that 2 are running in each AZ. If one AZ fails, the remaining two AZs can still operate with at least 4 machines.  
Option 1 is incorrect. By setting a cooldown, you may be able to better manage your costs, but you will not be able to maintain your SLA as this is not a feature that will allow you to maintain at least 4 EC2 instances.  
Option 2 is incorrect. Changing instance types is a way to optimize performance and has nothing to do with maintaining an SLA.  
Option 4 is incorrect. Since a total of 8 EC2 instances are running in 2 AZs, we can see that 4 are running in each AZ. Even if one AZ fails, at least 4 units can be operated in the remaining AZs. This is not suitable as it will

1. 26. Question

You are designing the AWS architecture so that you can access internal business systems from mobile terminal applications. As a requirement, there is an upload of business data from the mobile terminal application to S3.  
However, there are concerns that a large amount of traffic will be generated if mobile terminal applications upload data via a web application server built on AWS.  
What is the most cost efficient and appropriate way to upload data from mobile device applications to Amazon S3?

* + Take advantage of Amazon S3‘s cross-region replication feature
  + **Upload data to a temporary separate bucket on Amazon S3 and have AWS Lambda function copy to appropriate S3 bucket after completion**
  + Increase web server instance size to handle large amounts of traffic
  + **Publish presigned URLs for Amazon S3 and upload data directly from mobile device applications**

**Incorrect**

With Amazon S3, you can issue signed URLs using the AWS CLI or AWS SDK.  
Presigned URL is a function to issue a URL to allow access to S3 for a certain period of time. Users and applications that are not logged in to AWS can directly access or write data on S3. can be given access to You can freely decide the access time, so you can send and receive secure files.  
Option 1 is incorrect. Data stored in S3 is automatically replicated to 3 AZs in the same region by default, but by enabling cross-region replication, objects are automatically replicated to an S3 bucket in another region. . Not suitable due to S3‘s fault tolerance features.  
Option 2 is incorrect. It is not suitable because it does not solve the point of relaying the Web server and generating a large amount of traffic.  
Option 3 is incorrect. Increasing the web server instance size is likely to increase costs, so it is not an efficient method in this case.

1. 27. Question

Your company has a large Microsoft SharePoint on-premises that requires Windows shared file storage.  
You want to move this workload to AWS and are considering various storage options. Storage should be highly available and integrated with Active Directory for access control. Which of the following is an appropriate way to meet these requirements?

* + **Use Amazon EFS storage and set up an Active Directory domain for authentication**
  + Create a file gateway for AWS Storage Gateway with SMB file sharing across two Availability Zones (AZs)
  + Create an S3 bucket and mount it as a Windows Server volume
  + **Create Amazon FSx for Windows as a file server on AWS and configure an Active Directory domain for authentication**

**Incorrect**

Amazon FSx for Windows is reliable, scalable, fully managed file storage that can be integrated with your on-premises Active Directory or AWS Managed Microsoft AD for access control.  
Option 1 is incorrect. Amazon EFS accesses via NFS, so it cannot be used as Windows shared file storage.  
Option 2 is incorrect. The ability of the AWS Storage Gateway service alone does not allow you to configure your instances in two Availability Zones (AZs).  
Option 3 is incorrect. Amazon S3 does not come standard with the ability to mount on Windows servers.

1. 28. Question

A company operates an application that uses its own file system on a legacy server that is used in a legacy system. Which storage service should you use when migrating legacy servers to AWS?

* + **Amazon EBS**
  + Amazon EFS
  + **Amazon S3**
  + Amazon S3 Glacier
  + Amazon DynamoDB

**Incorrect**

Amazon EBS is a persistent block storage service, available by attaching it to an EC2 instance. Since it is a block storage device, any file system can be created from the OS hosted on EC2.  
Option 2 is incorrect. Amazon EFS is a scalable shared storage service. EFS provides NFS functionality and currently only supports Linux file systems. Available from multiple EC2 instances (Linux).  
Option 3 is incorrect. Amazon S3 is an object storage service.  
Option 4 is incorrect. Glacier is a storage service aimed at archiving.  
Option 5 is incorrect. Amazon DynamoDB is a NoSQL managed database.

1. 29. Question

A company has a campaign site that consists of three layers of web applications. The campaign site is distributed on EC2, and the database uses Amazon RDS (Aurora).  
With a spike in traffic expected over the weekend, which design will not overload RDS and minimize costs?

* + Configure an Auto Scaling group on EC2
  + **Configure Amazon DynamoDB Accelerator (DAX) to cache on database reads**
  + Configure Amazon DynamoDB to handle traffic spikes
  + **Configure Auto Scaling on RDS database instances**
  + Configure multiple RDS database instances in advance

**Incorrect**

Aurora‘s Auto Scaling allows you to monitor resource usage and automatically increase or decrease RDS database instances based on that usage.  
Option 1 is incorrect. Auto Scaling is possible with EC2 as well, but it doesn‘t reduce the load on RDS.  
Option 2 is incorrect. Since Amazon DynamoDB is a NoSQL database, it cannot replace the RDS database, which is a relational database.  
Option 3 is incorrect. Since Amazon DynamoDB is a NoSQL type database, it cannot replace the RDS database which is a relational type database.  
Option 5 is incorrect. There is no cost advantage to creating multiple RDS instances in advance.

1. 30. Question

There is an image sharing site for specific members using Amazon S3. It was reported that an unspecified number of non-members accessed this site and downloaded images. How can you resolve this situation? (Choose 2)

* + **Use signed URLs with expiration**
  + **Since Amazon S3 cannot share images only with members, save photos in the EBS volume of the web server**
  + Use security groups to allow access only to members‘ IP addresses
  + **Remove Amazon S3 public access**

**Incorrect**

By using a signed URL with an expiration date, you can allow users to download files only for a certain period of time by notifying them of this URL.  
By using Amazon S3, you can easily publish files to the outside, but if you do not set it properly, you will allow access from unexpected users.  
S3 has an access control feature called public access. If you don‘t want the file to be open to the general public, don‘t set this permission. By setting appropriate permissions on S3, you can securely grant specific users access to your files.

1. 31. Question

A company has a two-tier web application running in public and private subnets. The application tier runs in a public subnet and the database tier runs in a private subnet, both running on EC2 instances in a single Availability Zone (AZ).  
Which of the following methods should be combined to achieve high availability in this architecture (choose two)?

* + Create new public and private subnets in the same AZ
  + **Create an EC2 Auto Scaling Group and Application Load Balancer Across Multiple AZs**
  + **Add an existing web application instance to an Application Load Balancer Auto Scaling group**
  + Create new public and private subnets in separate AZs and build database tier on EC2 instances in one AZ
  + **Create new public and private subnets in separate AZs and migrate the database to a multi-AZ deployment on Amazon RDS**

**Incorrect**

The two-tier web application in question is running on EC2 instances running in a single Availability Zone (AZ) for both the application and database tiers. In order to “realize high availability“ as asked in the question, the point is to perform geographically distant redundancy.  
You can achieve geographically distant redundancy by auto scaling your EC2 instances across multiple AZs. Also, by combining with Application Load Balancer (ALB), communication can be distributed appropriately even if an EC2 instance fails.  
In addition, by deploying Amazon RDS multi-AZ for the database layer, geographically separated redundancy across AZs can be achieved, and high availability can be achieved by automatically switching over even if a failure occurs. .  
Option 1 is incorrect. Even if subnets are created in the same AZ, geographically separated redundancy across AZs cannot be achieved.  
Option 3 is incorrect. Since the existing web application is running in a single AZ, combining ALBs does not provide cross-AZ redundancy.  
Option 4 is incorrect. Even if you create a new subnet in another AZ, you won‘t be able to achieve high availability if your EC2 instances are running in a single AZ.

1. 32. Question

A company uses a Windows server as a shared file server within the company. Windows folder sharing and replication between multiple Windows servers (DFS replication) are realized using the SMB protocol.  
As a solution architect, you would like to reduce construction and operation costs by migrating this file sharing mechanism to AWS. Which AWS service is a good migration destination?

* + Amazon EFS
  + Amazon S3
  + **Amazon FSx for Windows**
  + Amazon EBS
  + Amazon FSx for Luster

**Correct**

This question asks you to select an appropriate AWS service when migrating a Windows server file sharing mechanism.  
Amazon FSx for Windows is a fully managed, reliable, and scalable file storage service accessible via the SMB protocol standard for Windows file sharing. Built on Windows Server, it offers a wide range of standard Windows Server management features such as quotas and Microsoft Active Directory integration.  
Option 1 is incorrect. Amazon EFS provides NFS functionality and can be used from multiple EC2 instances, but it does not meet the requirements of the question.  
Option 2 is incorrect. Amazon S3 is an object storage service.  
Option 4 is incorrect. Amazon EBS is a persistent block storage service available by attaching it to an EC2 instance.  
Option 5 is incorrect. Amazon FSx for Luster is a fully managed service that allows you to use the high-performance Luster file system.

1. 33. Question

You would like to build a system on AWS that connects to Amazon DynamoDB from an application within a VPC. However, your application and DynamoDB are not allowed to connect over the internet, so you must have a private connection within the same region.  
Which of the following is the appropriate service to use in this situation?

* + VPC peering
  + AWS Direct Connect
  + **NAT gateway**
  + **VPC endpoint**

**Incorrect**

A VPC endpoint is a service that enables private connections within AWS without going through the Internet when accessing Amazon S3 or Amazon DynamoDB. It is available by setting a target to the specified route in the route table.  
Option 1 is incorrect. VPC Peering is a service that provides a private connection between different VPCs, and does not create a connection path to AWS services.  
Option 2 is incorrect. AWS Direct Connect is a service that connects the on-premises environment and AWS with a dedicated line, so it does not create a connection path to AWS services.  
Option 3 is incorrect. A NAT gateway is a NAT service for connecting EC2 instances in private subnets to the Internet. You can create a route to an AWS service, but it will be over the Internet.

1. 34. Question

A company builds web applications and operates services for the Internet. This web application consists of Amazon Cloud Front, Application Load Balancer, and EC2, with Application Load Balancer set as the origin server for CloudFront.  
Malicious attacks from a specific IP address have recently been detected from access logs. Which solution blocks specific IP addresses for future security measures?

* + **Block access from a specific IP address with an EC2 security group under Application Load Balancer**
  + **Set AWS WAF to Amazon CloudFront and block access from specific IP addresses using WAF‘s IP address match conditions**
  + Block access from specific IP addresses with EC2 network ACL under Application Load Balancer
  + Block access from specific IP addresses in Amazon CloudFront settings

**Incorrect**

Using AWS WAF is a good way to block malicious attacks from the Internet through specific IP addresses.  
AWS WAF is a web application firewall that can be set up on Amazon CloudFront, etc. You can create security rules that block common attack patterns such as SQL injection and cross-site scripting, or rules that exclude specific predefined traffic patterns such as IP addresses.  
In the question, CloudFront is used for the Internet, and AWS WAF can be set to block specific IP addresses for CloudFront. So option 2 is the correct answer.

1. 35. Question

Your company needs to migrate 20TB of data from its data center to the AWS cloud within 30 days due to system renewal. Network bandwidth is limited to 15Mbps and usage cannot exceed 70%.  
Which of the following services should be used to meet these requirements?

* + **Migrate data using AWS Snowball**
  + Migrate data using AWS DataSync
  + Migrate data using File Gateway of AWS Storage Gateway
  + **Migrate data to Amazon S3 using Amazon S3 Transfer Acceleration**

**Incorrect**

With AWS Snowball, the migration data is stored in the Snowball enclosure shipped from AWS, and when the enclosure is returned to AWS, AWS will migrate the data. It is ideal for migrating large amounts of data when network bandwidth is limited, as in your question.  
Option 2 is incorrect. Since AWS DataSync transfers data over the network, it may be difficult to migrate data within the limited network bandwidth.  
Option 3 is incorrect. AWS Storage Gateway makes it appear that the server and Amazon S3 are connected locally, but actually transfers data over the network. Therefore, it is considered difficult to transfer data within the time limit while the network bandwidth is limited.  
Option 4 is incorrect. Amazon S3 Transfer Acceleration is a service that uses edge locations to optimize data transfers to S3. Data transfer must go through the Internet, and it is considered difficult to migrate data within the deadline due to network bandwidth limitations.

1. 36. Question

Since the application you are developing is a global service, you know that there will always be a lot of reads and writes to the database. You do not want the database to become a bottleneck in this application.  
Which of the following EBS storage types can maximize application performance without introducing database-side processing bottlenecks?

* + **Provisioned IOPS SSD**
  + **Throughput optimized HDD**
  + Cold HDD
  + General-purpose SSD

**Incorrect**

Databases that require high read and write performance generally should choose a storage type that can deliver low latency and high throughput performance. Provisioned IOPS SSDs have the highest performance and are often used for mission-critical databases.  
Option 2 is incorrect. Throughput Optimized HDDs are HDDs with high throughput and low cost. It is suitable for storing frequently accessed data such as big data storage and log processing.  
Option 3 is incorrect. A cold HDD is suitable for storing large amounts of infrequently accessed data. It is also suitable if you want to be more cost effective.  
Option 4 is incorrect. General Purpose SSD is an EBS storage type that strikes a good balance between price and performance.

1. 37. Question

A gaming company builds multiple EC2 instances in a single Availability Zone (AZ) to run a multiplayer game that communicates with users at Layer 4. The gaming company wants their architecture to be highly available and cost effective.  
As a solution architect, what design changes should you recommend to meet this requirement? (Choose 2)

* + **Increase number of EC2 instances**
  + Reduce number of EC2 instances
  + **Configure Network Load Balancer in front of EC2 instances**
  + **Configure Application Load Balancer in front of EC2 instances**
  + **Configure an Auto Scaling group to automatically add or remove EC2 instances across multiple AZs**

**Incorrect**

Since it is a system that communicates at Layer 4, it is expected that the availability of multiple EC2 instances that are currently being constructed can be improved by configuring a Network Load Balancer (Option 3).  
Deploying EC2 instances across multiple Availability Zones can increase availability and Auto Scaling can be cost effective (Option 5).

1. 38. Question

Your company builds applications for customer companies on AWS. The images used in the application are stored in the RDS MySQL database, but the number of images is increasing day by day, and the number of accesses to images is also very high, so you were asked to implement measures to reduce costs and improve performance. Which of the following is the appropriate response?

* + Using read replicas of MySQL databases on Amazon RDS
  + Only 10% of image files that are used particularly frequently are stored in the Amazon RDS MySQL database, and the rest are migrated to Amazon S3 Glacier.
  + **Migrate all image files to Amazon EBS and allow customers to access images through Amazon CloudFront**
  + **Migrate all image files to Amazon S3 and allow customers to access images via Amazon CloudFront**

**Incorrect**

AWS has a CDN (Content Delivery Network) service called CloudFront. By using this service, it is possible to deliver content such as images and videos safely and at high speed. CloudFront can cache web content such as video files as well as image files, which are static content as in the question. You can also keep costs down by storing image files in Amazon S3.  
Option 1 is incorrect.  
Due to the sheer volume of data across multiple applications, AWS Direct Connect may not be able to complete the first data migration in less than a month.  
Option 2 is incorrect. Similarly, with a Site to Site VPN, the initial data migration may not be completed within a month, and it may be difficult to maintain stable throughput after the migration.  
Option 3 is incorrect. AWS Snowball is very effective as a means of transferring large amounts of data to AWS at once. Even after migration, Direct Connect can be expected to maintain secure and stable throughput, but it is difficult to maintain stable throughput with Site to Site VPN.

1. 39. Question

Which of the Amazon Aurora features is incorrect?

* + managed service
  + **Higher throughput than MySQL and PostgreSQL**
  + Highly durable as data is stored across 3 Availability Zones (AZs)
  + **Column-oriented architecture suitable for aggregation and analysis of large amounts of data**
  + is a relational database service

**Incorrect**

Amazon Redshift is a service that has a column-oriented architecture and is suitable for aggregation and analysis of large amounts of data. So option 4 is wrong and is the correct answer.

1. 40. Question

Your company operates a web service. A web application server connects to a database located in a private subnet within the VPC.  
As a solution architect, you must design according to the following security requirements for enhanced security.  
?The web application server accepts SSL (HTTPS connections) from the Internet.  
?The database server only accepts connections from the web application server  
Which security settings would have the least impact on live services? (choose two)

* + Network ACL to allow all inbound communication and deny all outbound communication for HTTPS connections to the subnet of the web application server
  + **In the security group, open the database server connection port and only allow connections from the web application server security group**
  + Relocate the database server to the same subnet as the web application server
  + **Network ACL to allow all inbound communication and deny all outbound communication to the connection port of the database server for the private subnet**
  + **Open the HTTPS port of the web application server and allow connections from the Internet (0.0.0.0/0) in the security group**

**Incorrect**

By using security groups, firewall functions are provided for each of the web application server and database server.  
Network ACL, on the other hand, is a firewall function that is set for each subnet. Unlike security groups, they are stateless, so you need to explicitly control inbound and outbound communication. If network ACLs deny all outbound communication for the web application server and database server subnets, return communication is not possible (options 1 and 4).  
Simply placing the web application server and database server on the same subnet does not meet security requirements (option 3).

1. 41. Question

A company runs a web application on-premises. The web application is containerized and running on multiple Linux hosts connected to a PostgreSQL database containing user records.  
The company found that the operating costs of maintaining infrastructure and planning for future capacity were a hindrance to its growth. Which action should the Solution Architect take to resolve this issue?

* + **Migrate PostgreSQL database to Amazon Aurora**
  + Host your web application on an EC2 instance
  + **Distributing web application content using Amazon CloudFront**
  + Place Amazon ElastiCache between your web application and your PostgreSQL database

**Incorrect**

By using Amazon CloudFront to cache content in edge locations, you can distribute content in a scalable manner. Also, because CloudFront is a managed service, there are no operational costs associated with containers.  
Option 1 is incorrect. While migrating your database to Amazon Aurora solves the operational cost and capacity planning issues, you also need to do the same on the container side where your application is running.  
Option 2 is incorrect. Hosting your web application on an EC2 instance won‘t solve the problem, as you‘re not using a managed service, and you‘ll need to do maintenance and capacity planning.  
Option 4 is incorrect. By caching database queries in Amazon ElastiCache, performance improvement for database access can be expected, but the number of resources to be operated will increase, making it difficult to reduce operating costs.

1. 42. Question

A company stores monthly attendance record data as PDF files in an S3 bucket. The general affairs department frequently accesses attendance record data for the previous month. You don‘t access the past attendance record data much more than the previous month‘s, but You need to get the data as soon as possible.  
The company has many employees and is looking to reduce the cost of storing data in S3 buckets.  
What is the most cost-effective and durable way to store time and attendance data in an S3 bucket?

* + Manually archive historical attendance record data to Amazon S3 Glacier on a regular basis
  + **Migrate past data from the previous month to Standard-Infrequent Access by setting Amazon S3 lifecycle rules**
  + Migrate past data from the previous month to One Zone-Infrequent Access by setting Amazon S3 lifecycle rules
  + Convert attendance record data to binary and save to Amazon RDS

**Correct**

Standard-Infrequent Access has the same level of durability as the standard class, and the data storage cost is lower than the standard class. However, because you are charged for reading the data, it is suitable for infrequently accessed data.  
Option 1 is incorrect. Archival storage such as Amazon S3 Glacier is not suitable because past data must be retrieved as soon as it is needed.  
Option 3 is incorrect. One Zone-Infrequent Access stores data in only one Availability Zone (AZ). Costs can be reduced by approximately 20% compared to the standard class, which replicates data across multiple AZs. It is suitable when the data is accessed infrequently, does not require high durability, and you want to retrieve it as soon as necessary, but it is not suitable when durability is required.  
Option 4 is incorrect. Converting data to binary and storing it in Amazon RDS requires additional AWS resources such as RDS database instances, which is not suitable from a cost perspective.

1. 43. Question

You need to establish IPv6 traffic to the internet from an EC2 instance in a private subnet. It should also scale automatically and not incur additional costs.  
Which of the following services meets this requirement?

* + **Egress-Only Internet Gateway**
  + NAT gateway
  + custom NAT instance
  + VPC endpoint

**Correct**

Egress-Only Internet Gateway is a redundant gateway that allows you to connect from your VPC to the Internet using IPv6.  
Option 2 is incorrect. A NAT gateway is a redundant gateway that connects a private subnet to the Internet, but charges are incurred according to the usage time.  
Option 3 is incorrect. Custom NAT instances use EC2 instances as NAT servers and cannot be automatically scaled.  
Option 4 is incorrect. VPC endpoints have the function of privately connecting to various AWS services and cannot connect to the Internet.

1. 44. Question

You are considering introducing Amazon S3 as a storage destination for business data that includes confidential information owned by your company. Security requirements are stringent, requiring encryption of stored data, automatic rotation of encryption keys, visualization and trail management of encryption key usage, and authority management of encryption keys.  
Which of the following is a good way to achieve these requirements with S3?

* + **Create an S3 bucket to manage encryption keys with the AWS KMS service and use server-side encryption (SSE - KMS)**
  + **Create an S3 bucket to use server-side encryption (SSE S3) with encryption keys managed by Amazon S3. Also, enable the file versioning function in the S3 bucket**
  + Create an S3 bucket to use server-side encryption (SSE S3) with encryption keys managed by Amazon S3
  + Create an S3 bucket to use server-side encryption (SSE-C) with company-issued and controlled encryption keys

**Incorrect**

There are three ways to encrypt bucket objects in Amazon S3:  
? AES-256 encryption using S3‘s default key  
? AES-256 encryption with keys managed by AWS Key Management Service (AWS KMS)  
? AES-256 encryption with user‘s arbitrary key  
The problem requires automatic rotation of encryption keys, visualization and trail management of encryption key usage, and key authority management. Option 1 is the correct answer, as encryption powered by AWS KMS can achieve these capabilities.

1. 45. Question

It turned out that the web server was being accessed illegally from a specific IP address. If You want to deny connections from this IP address, what service or feature should you use?

* + **internet gateway**
  + **network ACLs**
  + AWS Direct Connect
  + Amazon API Gateway

**Incorrect**

Network ACL is a firewall function for subnets configured in VPC, and can control access from specific IP addresses.  
Option 1 is incorrect. The internet gateway is a gateway for accessing the internet from resources within the VPC, and is not for access control.  
Option 3 is incorrect. AWS Direct Connect is a service that connects the on-premises environment and AWS with a dedicated line.  
Option 4 is incorrect. Amazon API Gateway is a service that makes it easy to create, distribute, maintain, monitor, and secure APIs, not access control.

1. 46. Question

A large global application is being built for use in the US, Europe, and Japan, and you, the solution architect, have been asked about a database. The requests from the company are as follows.  
?The database should be distributed in multiple regions so that high-speed processing can be performed even if the application is used in each country.  
?When data is written in each region, the changes must be reflected in distributed tables in other regions. Also, the change should be reflected within about 1 second.  
?In the event that conflicts arise when the same item in the table is updated simultaneously in each region, the content of the last updater should be reflected.  
Which solution can meet these demands?

* + **Choose Amazon ElastiCache for the database and Redis for the data store**
  + Select Amazon Redshift for the database and build a cluster with 3 or more computer nodes
  + Choose Amazon Aurora for your database and use read replicas
  + **Choose Amazon DynamoDB as your database and use global tables**

**Incorrect**

Amazon DynamoDB global table is a fully managed solution that maintains data consistency in database tables located in multiple regions.  
Unlike read replicas, DynamoDB global tables do not have one master table that synchronizes its data to other replica tables. Since all tables are master tables, data changes to tables in any region are synchronized with tables in other regions.  
New writes and updates to data typically occur within a second and are reflected in other distributed tables. Updates may occur at approximately the same time and conflicts may occur, in which case the last update will be reflected.  
Option 1 is incorrect. Amazon ElastiCache is a key-value NoSQL database service. It is generally used to improve the performance of RDS.  
Option 2 is incorrect. Amazon Redshift is a managed data warehouse service capable of handling petabytes of data. Since data is distributed by increasing the number of computer nodes, it is suitable for aggregation and analysis of large amounts of data.  
Option 3 is incorrect. An Amazon Aurora read replica replicates the same database as the master database and is constructed as read-only. It is used to improve the performance of data read operations.

1. 47. Question

Your company runs a website on EC2 instances registered with an Application Load Balancer and uses Amazon Route 53 for DNS.  
The company wants to build a backup site that users can access if their main website goes down.  
Which of the following solutions best meets these requirements?

* + **Use Amazon S3 website hosting as a backup site and configure Amazon Route 53 failover routing policy**
  + Use Amazon S3 website hosting for backup site and set Amazon Route 53 latency routing policy
  + **Deploy your application to another region and use ELB health checks for failover routing**
  + Deploy the application in another region and set up a redirect on the server side of the main site

**Incorrect**

By setting Amazon Route53 failover routing to Amazon S3 website hosting, it is possible to automatically switch to a backup site when a failure is detected at the main site.  
Option 2 is incorrect. If you set the latency routing of Route 53, it will connect to the site with low latency, so it may connect to the backup site even if the main site is running.  
Option 3 is incorrect. ELB can be redundant across Availability Zones (AZ), but it cannot be redundant across regions.  
Option 4 is incorrect. If the main site server goes down, the server will not accept access from users and will not be able to redirect to the backup site.

1. 48. Question

Your company has an application running on EC2 instances and you want to attach an IAM role to set access control to Amazon DynamoDB.  
The DynamoDB table name to be accessed is users and you would like to only allow deletion of records in the users table from EC2.  
Which of the following IAM policies follows the law of least privilege?

* + {  
       “Version“:“2012-10-17“,  
       “Statement“:[  
          {  
                “Effect“: “Allow“,  
                 “Action“: “dynamodb:DeleteItem“,  
                 “Resource“: “arn:aws:dynamodb:ap-northeast-1:xxxxxxxxxxxx:table/\*“,  
           }  
        ]  
    }
  + **{  
       “Version“:“2012-10-17“,  
       “Statement“:[  
           {  
                 “Effect“: “Allow“,  
                 “Action“: “dynamodb:DeleteItem“,  
                 “Resource“: “arn:aws:dynamodb:ap-northeast-1:xxxxxxxxxxxx:table/users“,  
           }  
        ]  
    }**
  + {  
       “Version“:“2012-10-17“,  
       “Statement“:[  
           {  
                 “Effect“: “Allow“,  
                 “Action“: “dynamodb:\*“,  
                 “Resource“: “arn:aws:dynamodb:ap-northeast-1:xxxxxxxxxxxx:table/\*“,  
           }  
        ]  
    }
  + {  
       “Version“:“2012-10-17“,  
       “Statement“:[  
          {  
                 “Effect“: “Allow“,  
                 “Action“: “dynamodb:\*“,  
                 “Resource“: “arn:aws:dynamodb:ap-northeast-1:xxxxxxxxxxxx:table/users“,  
          }  
        ]  
    }

**Correct**

Create an IAM policy with Delete Record permission only for the users table in Amazon S3 DynamoDB and associate it with the IAM role.  
The correct option is option 2, which allows the action to delete records only in the DynamoDB table and specifies only the DynamoDB users table as the target resource.  
Option 1 is incorrect. The target table is “\*“ and the range is too wide.  
Option 4 is incorrect. It violates the law of least privilege because it allows all actions in DynamoDB.  
Option 3 is incorrect. This is incorrect because it includes both option 1 and option 4.

1. 49. Question

A company separates its batch processing systems into two. One is batch processing that is executed on mission-critical core systems, and the other is batch processing that is executed on non-core systems that do not directly affect business operations.  
These batch processes are run on an irregular basis. Which of the following would be a good configuration to build this system at as low a cost as possible?

* + Configuring a core system as a Reserved Instance and a non-core system as an On-Demand Instance
  + **Configure core systems with Reserved Instances and non-core systems with Spot Instances**
  + Configure on-demand instances for both core and non-core systems
  + Configure core systems with Spot Instances and non-core systems with Reserved Instances

**Unattempted**

Reserved Instances are suitable for batch processing that runs on mission-critical systems, because instances need to be started all the time.  
On the other hand, batch processing performed on non-core systems does not directly affect operations even if the processing is interrupted, so the lowest cost Spot Instance is appropriate.

1. 50. Question

You belong to the information systems department at the headquarters of a company with branch offices in Asian countries.  
At the company‘s management meeting, meetings are held using the business data accumulated in Redshift every day, so you are preparing the analysis results of the previous day‘s data. Although this analysis requires many queries, each branch usually has enough time to store the data and analyze it. Also, due to the time difference, Redshift query processing can be executed without any problems. However, depending on the situation at the branch office, in rare cases, data storage to Amazon Redshift may be slow.  
Even in such cases, it is necessary to reliably provide analysis results, so when the number of Redshift queries increases, you would like to be able to scale and process according to the number of queries.  
Which of the following is the correct solution?

* + Store pending queries in SQS
  + Take advantage of cross-region snapshots
  + increase the number of nodes
  + **Enable Redshift concurrency scaling**

**Unattempted**

When Amazon Redshift has a large number of concurrently executing queries, queries that cannot be processed are stored in a queue, and waiting time occurs until resources are secured for processing in Redshift.  
However, with Redshift concurrency scaling enabled, Redshift will automatically scale and process queries within a pre-set range when bursty use cases occur.  
Option 1 is incorrect. Even without using SQS, pending Redshift queries are stored in a Redshift queue. Also, storing in a queue does not allow multiple queries to be executed quickly.  
Option 2 is incorrect. Cross-region snapshots are a feature that allows you to replicate a snapshot to a region other than where the cluster is located when the snapshot is taken. This feature is intended for backup purposes and is not appropriate for the case in question.  
Option 3 is incorrect. Increasing the number of Redshift nodes may speed up data storage and query processing, but it is not possible to scale and process queries according to the number of processes.

1. 51. Question

You are building an application that runs on an EC2 instance and wants to use Amazon DynamoDB as your database. This application must be able to write data to DynamoDB from an EC2 instance.  
Which of the following (choose two) best describes when the key pair (access key ID and secret access key) is not allowed to be stored on the EC2 instance?

* + **Create an IAM role that allows writing to Amazon DynamoDB**
  + Writing to Amazon DynamoDB is possible without IAM role permissions
  + Add an IAM User to a Running EC2 Instance
  + **Launch an EC2 instance with an IAM role included in the Auto Scaling launch configuration**

**Unattempted**

To use Amazon DynamoDB from an EC2 instance, you need privileges according to the functions you use.  
In the case of the question, to write to DynamoDB from the EC2 instance, create an IAM role that allows writing to DynamoDB for the EC2 instance. Also, if you use Auto Scaling, set the above IAM role in your launch configuration.

1. 52. Question

You are designing a web application that is required to run only 7 hours a day on an EC2 instance. This EC2 instance works stably using the r4.8xlarge instance type. This system does not require high availability and will be retired after a year.  
What would be the most cost effective purchasing option for EC2 to power this system?

* + Standard type Reserved Instance
  + Convertible type Reserved Instance
  + **Scheduled Reserved Instance**
  + spot instance

**Unattempted**

A Scheduled Reserved Instance is a purchase option that allows you to launch within a reserved time window and is billed for the time the instance is scheduled. It is suitable for periodic processing that does not need to be performed continuously, such as batch processing that is performed on non-business days. Therefore, it is a good purchase option for the system in question, which only runs 7 hours a day.  
Options 1 and 2 are incorrect. In the case of the question, Standard type Reserved Instances and Convertible type Reserved Instances are not suitable because they only need to run for 7 hours every day.  
Option 4 is incorrect. Also, Spot Instances are not suitable either, as high availability is not required, but 7 hours of operation is required.

1. 53. Question

Your company has an on-premises server running a relational database. Today‘s databases generate high read traffic from users in many different locations.  
You want to migrate your database server to AWS with minimal changes. You need to be able to continue your business in the event of a database failure and not be affected by current traffic.  
Which solution meets these requirements?

* + Build a database hosted on EC2 instances registered to an Application Load Balancer in different Availability Zones (AZs)
  + Build a database hosted on multiple EC2 instances in different regions
  + **Use Amazon RDS and configure with a Multi-AZ deployment and one or more read replicas**
  + Use Amazon RDS and configure with a Multi-AZ deployment and one or more standby databases

**Unattempted**

In the case of the question, we can expect to improve fault tolerance with Amazon RDS Multi-AZ and improve read throughput with read replicas.  
Options 1 and 2 are incorrect. Placing databases in different Availability Zones (AZs) or regions improves business continuity, but if you want to configure database redundancy with EC2 instances, you will need to introduce a clustering mechanism, and the configuration will be large. It may be necessary to reconsider.  
Option 4 is incorrect. RDS does not have the ability to configure a standby database.

1. 54. Question

You are architecting a new application that requires low network latency and high network throughput across EC2 instances.  
Which is the correct solution to choose to achieve this?

* + AWS Auto Scaling
  + **Cluster Placement Group (Cluster Placement Group)**
  + Partition Placement Group (Partition Placement Group)
  + Spread Placement Group (Spread Placement Group)

**Unattempted**

A placement group is a logical grouping of EC2 instances.  
By grouping using the placement group function, communication between the grouped EC2 instances becomes even faster than normal communication between EC2 instances.  
By placing EC2 instances in the same rack, a cluster placement group enables high-speed communication between instances, making it suitable for applications that require a network with low latency and high throughput.  
Option 1 is incorrect. AWS Auto Scaling is a service with automatic scaling and predictive scaling capabilities.  
Option 3 is incorrect. Partition placement groups place EC2 instances in different racks by partition. Suitable for distributed processing.  
Option 4 is incorrect. A spread placement group places all EC2 instances in different racks. Suitable for systems that want to reduce the impact of failures.

1. 55. Question

You are designing an internal shared file system that is always accessible. Each team has its own independent directory and wants to protect the files so that users can only access files owned by their team.  
Which of the following is a good design strategy?

* + **Use Amazon EFS and perform access control on a file-by-file basis**
  + Access control by ACL using Amazon S3
  + Use Amazon S3 and perform access control by IAM
  + Use Amazon EFS and perform access control by security group

**Unattempted**

Amazon EFS is used by mounting it to an EC2 instance. Therefore, it is possible to control access to files using OS functions.  
Option 2 is incorrect. Amazon S3 can control access with ACLs, but AWS accounts and public access are targeted, and it is not possible to control with user groups.  
Option 3 is incorrect. When performing access control with IAM, API calls are targeted, and access control for each directory cannot be performed.  
Option 4 is incorrect. Security groups cannot provide per-directory access control.

1. 56. Question

Which of the following is a good way to access Amazon S3 from EC2 instances in private subnets without going over the internet?

* + Create a VPC endpoint for your EC2 instance and set an Amazon S3 target in your route table
  + Create a VPC endpoint interface for your EC2 instance
  + **Create a VPC endpoint for Amazon S3 and set the Amazon S3 target in the route table**
  + Create a VPC endpoint interface for Amazon S3

**Unattempted**

To privately connect to Amazon S3 from an EC2 instance in a private subnet, create a gateway-type VPC endpoint and set the S3 target in the route table.  
A gateway-type VPC endpoint is provided for S3, and an interface-type VPC endpoint is provided for EC2.

1. 57. Question

Your company operates an internal file server that stores 100TB of business data. You are considering migrating data to Amazon S3 Glacier as a backup destination.  
Choose an appropriate migration method that is cost-effective while reducing strain on your internal network lines.

* + Upload files from a browser to S3 via the Internet. Lifecycle to archive data migrated on S3 to Glacier set the policy
  + Set up a site-to-site VPN between your company and your AWS VPC and upload files from your browser to Glacier over the VPN
  + Set up a site-to-site VPN between your company and your AWS VPC, and upload files from your browser to S3 via VPN. Set a lifecycle policy to archive data migrated on S3 to Glacier
  + **Use AWS Snowball and set an S3 bucket as the migration destination. Set a lifecycle policy to archive data migrated on S3 to Glacier**

**Unattempted**

Use AWS Snowball to archive large amounts of data to Glacier while avoiding line congestion. Snowball is a service that transfers large amounts of data to AWS internal storage. The housing used for Snowball is highly durable physically prepared by AWS, and it will be automatically shipped to the registered address simply by creating a job from the AWS management console.  
Data saved in Snowball is saved in S3, and it is necessary to set up archiving from S3 to Glacier.

1. 58. Question

A company publishes a static website using a Zone Apex called company.com. You want to use Amazon Route 53 for DNS for this website.  
Which of the following is a scalable and cost-effective configuration (choose two)?

* + Build a website on an EC2 instance and bind the public IP address of the EC2 instance as an Amazon Route 53 alias
  + Build a website using AWS CloudFormation and link the CloudFormation stack as an Amazon Route 53 alias
  + **Publish content on Amazon S3 with static website hosting and link S3 endpoints as Amazon Route 53 aliases**
  + **Build a website on EC2 using Elastic Load Balancing and Auto Scaling, and bind the Elastic Load Balancing endpoint as an Amazon Route 53 alias**

**Unattempted**

Aliases in Amazon Route 53 can configure Zone Apex records for Elastic Load Balancing (ELB) and Amazon CloudFront. Amazon Route 53, Amazon S3, ELB, and CloudFront are all AWS managed services, and you can combine them to configure your static website for cost-effective scalability according to load.  
Options 1 and 2 are incorrect.  
It cannot be bound to the public IP address of the EC2 instance or the CloudFormation stack.

1. 59. Question

For the purpose of web marketing, your company tracks each user‘s movement on the website and sends recommendations.  
You collect user access logs on EC2 instances in near real time and store them in Amazon RDS. Another EC2 instance checks the saved logs in real time and makes recommendations by SQL queries. As a solution architect, you want to decouple your current architecture and analyze real-time data with SQL. Choose the right solution.

* + After receiving access logs from the website using Amazon SNS, execute SQL queries from Lambda in cooperation with AWS Lambda
  + Use Amazon SQS to link data to the current EC2 instance after receiving access logs from the website
  + Use Amazon Kinesis Data Streams to save data to S3 with Amazon Kinesis Firehose after receiving access logs from the website. SQL analysis of stored data with Amazon Athena
  + **Use Amazon Kinesis Data Streams to receive access logs from websites and then perform SQL analysis with Amazon Kinesis Data Analytics. Store data in S3 with Amazon Kinesis Firehose**

**Unattempted**

Amazon Kinesis is a service that processes large amounts of data flowing in real time.  
Amazon Kinesis Data Streams, one of the Kinesis services, can collect streaming data in near real time, and the collected data can be saved to Amazon S3, Amazon RDS, etc. by Amazon Kinesis Data Firehose. Additionally, by working with Amazon Kinesis Data Analytics, you can run SQL queries on streaming data for real-time analysis.  
Options 1 and 2 are incorrect. Amazon SQS and Amazon SNS can be configured into a loosely coupled architecture, but Kinesis is better suited for real-time processing and SQL analysis.  
Option 3 is incorrect. It is possible to perform analysis after saving to Amazon Athena, but Kinesis is better suited for real-time requirements.

1. 60. Question

You have been consulted about system construction by a company that is considering providing services for B to C.  
This service does not always have access to the site, and it is expected that the number of users will increase rapidly only from evening to night in a day. You decide to use an EC2 Auto Scaling group to accommodate this temporary high load.  
As you proceeded with our research on other services, you found that a non-relational database was suitable for accumulating service user data, and that there was a demand for a mechanism that could automatically respond to changes in load. .  
Which of the following is the most appropriate solution to propose to this company?

* + Use Amazon Route 53 for traffic distribution and Amazon Aurora for data accumulation
  + Use Amazon Route53 for traffic distribution and Amazon DynamoDB for data accumulation
  + Use Network Load Balancer for traffic distribution and Amazon Aurora for data accumulation
  + **Use Network Load Balancer for traffic distribution and Amazon DynamoDB for data storage**

**Unattempted**

In the case of the question, it is required to be able to store data in a non-relational database and automatically respond to changes in load.  
For data storage, the managed NoSQL database service “Amazon DynamoDB“ is suitable. For load balancing, the load balancing service “Network Load Balancer“ that achieves high throughput with low latency is suitable.  
Options 1 and 3 are incorrect. Amazon Aurora is a relational database service, so it is not suitable for questions that require a non-relational database.  
Option 2 is incorrect. Amazon Route53 has a DNS failover feature that allows server switching in the event of a failure, but it is not suitable for the case in question.

1. 61. Question

Which of the following is an incorrect explanation regarding services and usage methods for using AWS securely?

* + Objects already stored in S3 can be encrypted using AWS KMS keys
  + **AWS KMS can manage created keys, but cannot disable or delete keys**
  + AWS CloudHSM is a customer-owned hardware appliance located within AWS data centers
  + AWS CloudHSM applies when security compliance requirements are stringent

**Unattempted**

AWS KMS is a managed service that provides key management on AWS, and can mainly create, enable/disable, rotate, and delete encryption keys.

1. 62. Question

Your company is designing a web application for image file sharing that is used by many members. You plan to use Amazon S3 to store the image files, but you would like to avoid increasing the traffic on the web server that goes through when uploading the image files.  
What is the best way to save images from this web application?

* + Fix the IP address of the web server using Elastic IP
  + Prepare multiple S3 buckets to temporarily store images. After the image is uploaded to the S3 bucket, the Lambda function moves the file to the S3 bucket for image storage.
  + By uploading to the Auto Scaling group using the ELB Classic Load Balancer, set it so that it can write to the S3 bucket
  + Use Spot Instances to extend the functionality of your web server to provide resources for image processing
  + **Upload directly to S3 using presigned URL**

**Unattempted**

Amazon S3 presigned URL is a function to issue a URL to allow access to data on S3 for a certain period of time. By using this function, files can be stored directly in S3 without going through a web server.

1. 63. Question

A company builds a web application and uses Amazon S3 for storage read from and written to by the application. Customers using the application have reported that they sometimes see outdated data, but you have confirmed that the functionality of the web application is working correctly. Which are the possible causes?

* + Web application is writing to Amazon S3 with multipart upload
  + **When writing to Amazon S3 from a web application, an existing file on S3 is overwritten and updated with the same object key**
  + A new file is created with a new object key each time the web application writes to Amazon S3.
  + Amazon S3 encryption function is enabled

**Unattempted**

Amazon S3 adopts an eventual consistency model when updating (PUT) or deleting (DELETE), and old data may be referenced depending on the timing of reference.  
Option 1 is incorrect. Multipart upload is a mechanism for efficiently transferring large objects to S3 by dividing them into multiple parts and uploading them.  
Option 3 is incorrect. In the case of new creation, instead of the eventual consistency model, after data is saved, data can be referenced when completion (HTTP200 response) is returned from S3, and data consistency is guaranteed.  
Option 4 is incorrect. Enabling or disabling the encryption feature is not a factor.

1. 64. Question

Your company operates an internal web application. It consists of two batch modules for front-end processing and back-end processing, and after receiving processing on the front-end, it is linked to back-end processing.  
This web application has a growing number of users and the backend processing is taking a long time. Therefore, you are considering migrating to Amazon ECS, making it a microservice, and creating an architecture that can withstand an increase in the number of users. Which of the following solutions is right for you?

* + **Use Amazon SQS to link front-end and back-end processing, and retrieve data from SQS queues**
  + Use Amazon SNS for coordination of front-end processing and back-end processing, and notify the topic of data
  + Use Amazon S3 for linking front-end processing and back-end processing, and trigger data registered in the S3 bucket
  + Use Amazon EFS to coordinate front-end and back-end processing and share data

**Unattempted**

The question asks how front-end and back-end processing work together. By using Amazon SQS, even when it is necessary to perform a large amount of processing or processing that takes a long time, it is possible to queue requests from the front-end processing in SQS and link and parallelize the processing to the back-end. I can do it.  
Option 2 is incorrect. Amazon SNS is a message notification service, but it is not suitable for processing coordination between microservices.  
Option 3 is incorrect. Amazon S3 is an object storage service.  
Option 4 is incorrect. Amazon EFS is a service that provides file sharing between EC2 instances, but it is not suitable from the viewpoint of processing coordination.

1. 65. Question

A service that distributes videos to members around the world has received complaints from members in some countries and regions that it takes a long time to play after accessing.  
Which of the following is a good way to reduce access-to-play time regardless of where you access it?

* + Store video files in Amazon S3 and access the URL directly
  + Store video files in Amazon S3 and use signed URLs
  + Start a web server on an EC2 instance and store video files on an EBS volume
  + **Use Amazon CloudFront signed URLs**

**Unattempted**

Amazon CloudFront is a CDN service that distributes content from globally distributed bases called edge locations. It has a highly available, high performance, low latency network.  
CloudFront signed URLs allow users to download and stream content.  
Video distribution is also possible by other methods, but Option 4 is the most suitable method for the question “Reduce the time from access to playback regardless of the region of access.“