1. 1. Question

You are publishing a web application composed of CLB and EC2. Which way to enable AWS WAF?

* + Enable AWS WAF with the current configuration.
  + **Enable AWS WAF by replacing CLB with ALB.**
  + Enable AWS WAF by replacing CLB with NLB.
  + Replace EC2 with ECS to enable AWS WAF.

**Correct**

AWS WAF is a web application firewall that can monitor HTTP(S) requests forwarded to AWS services that support this feature. The only load balancer type that supports AWS WAF is ALB (Application Load Balancer). CLB (Classic Load Balancer) is not compatible with AWS WAF and should be replaced with ALB. So option 2 is the correct answer.

1. 2. Question

Your company operates a website. When the server load suddenly increased, we checked the log and found that a large number of accesses were occurring from a specific address. As a temporary measure, how can I block these accesses as soon as possible?

* + Remove HTTP and HTTPS access from the inbound rules of the web server‘s security group.
  + Deny HTTP and HTTPS access from specific addresses in the inbound rules of the web server security group.
  + **Deny HTTP and HTTPS access from specific addresses in the network ACL of the public subnet.**
  + **Add settings to deny access from specific addresses to the OS firewalls of all web servers within the site.**

**Incorrect**

Network ACLs allow you to set deny rules from specific malicious addresses. Added deny rules apply to all servers in the subnet. You can continue to accept access from addresses that do not match the deny rules. So option 3 is the correct answer. Option 1 is incorrect. If you remove the security group inbound rules, even legitimate access will be blocked. Option 2 is incorrect. Security groups cannot be set to deny. Option 4 is incorrect. As a temporary workaround, deny rules in the network ACL are better in this case than making changes to all web servers.

1. 3. Question

Web applications exposed to the Internet must be highly available. An ELB is deployed in front of EC2 on the web tier. The database is deployed using RDS Multi-AZ. A NAT gateway is in place to access the Internet from your EC2 instance. The EC2 instance does not have a public IP address assigned. Which component is a potential single point of failure in this architecture?

* + **EC2**
  + **NAT gateway**
  + ELBs
  + RDS

**Incorrect**

In order to achieve high availability by eliminating a single point of failure in this configuration, it is necessary to install multiple EC2 units in each AZ. A single point of failure can be eliminated by adopting the configuration shown in Figure 8.2-9. So option 1 is the correct answer. Option 2 is incorrect. A NAT gateway is a service that implements redundancy within AWS zones. It is best to have redundancy across multiple zones, but if access frequency is low, there are cases where redundancy is only within a zone due to cost considerations. Option 3 is incorrect. ELBs are automatically redundant across AZs, so even if one unit goes down, the remaining ELBs can handle it. Option 4 is incorrect. Since the RDS is a multi-AZ configuration, even if the master RDS goes down, high availability can be achieved by promoting the slave RDS to master.

1. 4. Question

Your department operates using multiple EC2 as batch servers. We know that on certain days of the week, the nightly batch processing load is high, and we manually scale up EC2 to accommodate that particular day. The scaled up EC2 is supposed to be manually scaled down after work on the next business day. In the current operation, we are using an unnecessarily large size instance until we scale it down, and we are taking man-hours for work every week. You are looking for a cost-effective solution to solve this challenge. What should you do to meet these requirements?

* + **Take advantage of Auto Scaling. Enable the scaling strategy predictive scaling to increase or decrease the number of instances to accommodate the nightly batch processing window.**
  + **Use CloudWatch. Monitor EC2 CPU utilization and increase or decrease the number of instances with CloudWatch Events when the threshold is exceeded.**
  + Utilize Lambdas. Configure the Lambda function to run on a schedule, increasing or decreasing the number of instances according to the time period for nightly batch processing.
  + Use ECS. Migrate all batch applications on EC2 to ECS. Increase or decrease the number of instances in the ECS cluster settings.

**Incorrect**

Auto Scaling is a service that can automatically scale out and scale in EC2 under set conditions. You can set a scaling strategy, and when predictive scaling is enabled, machine learning automatically analyzes the load status history for up to 14 days and scales according to the demand forecast. As a result, when an increase in batch processing volume is detected on a specific day of each week, a scaling action is executed according to the batch processing time, and when the load decreases, scale-in is performed, so a cost-effective configuration can be achieved. So option 1 is the correct answer. Option 2 is incorrect. You can monitor CPU usage using CloudWatch, but you cannot increase or decrease the number of instances just by issuing CloudWatch Events. For scaling you need to combine Auto Scaling. Option 3 is incorrect. Lambda alone cannot scale out and scale in EC2 even if it is scheduled to run at a specific time. Option 4 is incorrect. Migrating batch applications on EC2 to ECS is labor intensive and not cost effective. Also, ECS clusters do not have a setting to enable auto scaling, so a combination with Auto Scaling is required.

1. 5. Question

Your company operates a mission-critical system on-premises. We are in the process of building a DR (Disaster Recovery) site on AWS to increase availability. I would like to migrate the data on-premises to the DR site on AWS over a few days. We have 15TB of data and our on-premises data center has a 1.5Gbps internet connection. Company security policy requires network encryption during data transfer. Which solution is the most appropriate from a cost perspective?

* + Lay a Direct Connect circuit between AWS and on-premises.
  + **Configure and connect VPN between AWS and on-premises.**
  + **Use FTP to transfer data from your on-premises server to AWS.**
  + Transfer data from on-premises servers to AWS using Kinesis.

**Incorrect**

Direct Connect and VPN connections can provide encryption at the network layer. However, in the case of the question, 15TB of data needs to be migrated within a few days, so Direct Connect, which takes time and money to install, is inappropriate. So, consider a VPN connection. You can set up a VPN connection between AWS and on-premises via the Internet line (1.5 Gbps) for secure data transfer. So option 2 is the correct answer. Option 1 is incorrect. As mentioned earlier, Direct Connect is inappropriate in this case. Option 3 is incorrect. It is possible to transfer data with FTP, but it must be encrypted at the network layer before that. Option 4 is incorrect. Kinesis is a service related to data streaming, Not suitable for row requirements.

1. 6. Question

You are designing storage for an application that stores the product drawing files you create and displays the saved drawings. A query to the database occurs to display the drawing. Cache query results to minimize database load time. Also, the created product drawing file must be archived for at least two years. The data size of product drawings to be archived is expected to be approximately 800TB in total. Archived files are accessed about once every few months. Which is the most cost-effective combination of storage and optimal caching services?

* + S3 and ElastiCache
  + S3 and CloudFront
  + EBS and CloudFront
  + **S3 Glacier and ElastiCache**

**Correct**

The question here is about cost-effective archival storage solutions and caching solutions when querying the database. S3 Glacier is suitable for cost-effective archival storage that is accessed once every few months, and ElastiCache is suitable for caching when issuing queries to the database. So option 4 is the correct answer. Option 1 is incorrect. It is also possible to store data in S3, but the cost is higher compared to S3 Glacier. Option 2 is incorrect. Like option 1, S3 has a higher cost compared to S3 Glacier. Also, CloudFront is effective as a cache for static content, but ElastiCache is more suitable for caching query results to the database for drawing display like this question. Option 3 is incorrect. The maximum size of EBS is 16TiB, which cannot store about 800TB of data.

1. 7. Question

You want to build a batch processing execution environment using Lambda. Batch processing is started when the file is saved to S3 or when the specified time comes. Batch processing consists of multiple steps, each step executing a Lambda function. I would like to perform conditional branching according to the processing result of the Lambda function so that if the processing of a step fails, exception handling is executed and the process is restarted from the first step. Which AWS service should I use in this case?

* + EMRs
  + SQS
  + **CodePipeline**
  + **Step Functions**

**Incorrect**

The Step Functions service allows you to write and execute a series of processing step flows using Lambda etc. Batch processing steps are triggered by storing files in S3 or CloudWatch events, and the Lambda function defined for each step is called to proceed with the process. So option 4 is the correct answer. Option 1 is incorrect. EMR is a service for big data processing. Lambda orchestration is not possible. Option 2 is incorrect. SQS is a queue service and cannot control branch processing. Option 3 is incorrect. CodePipeline is a CI/CD service for deploying developed programming code to the AWS environment. Batch processing step execution and branch processing cannot be performed.

1. 8. Question

Set up security groups in a three-tiered system like the one below. Web tier: Accept web access from users on the Internet. Associate the security group web-sg. Logic layer: A group of servers that execute RESTful APIs. Receives HTTPS access from Web layer servers and sends requests to the data layer. Associate the security group logic-sg. Data layer: PostgreSQL server. There is access using the 5432 port from the logic layer. Associate security group db-sg. Which is the correct combination of rules to set for each security group? (Choose 3)

* + **Add port numbers 80 and 443 from source 0.0.0.0/0 to web-sg inbound rules**
  + **Add port number 80 and 443 from source logic-sg to web-sg inbound rule**
  + Add port number 1024-65535 from source db-sg to logic-sg inbound rule
  + **Add port number 443 from source web-sg to logic-sg inbound rule**
  + **Add port number 5432 from source logic-sg to db-sg inbound rule**
  + Add port number 5432 from destination web-sg to db-sg outbound rule

**Incorrect**

Set according to your connection requirements. First, web-sg must allow inbound access for HTTP (port 80) and HTTPS (port 443) from the internet (all sources 0.0.0.0/0), so option 1 is the correct setup. Option 4 is the correct answer. Then logic-sg must allow inbound access for HTTPS (port 443) from the server web-sg is associated with (source security group web-sg). option 4 is the correct setting. Option 5 is the correct answer. Option 5 is the correct setup, because db-sg must allow inbound access to port 5432 from the servers that logic-sg is associated with (source security group logic-sg). Security group rules can specify a security group as the source. Note that security groups are stateful, so you don‘t need to configure outbound rules to allow responses for inbound traffic.

1. 9. Question

A company operates a Single Page Application (SPA) based music information website with customers around the world. The website consists of multiple EC2 instances load balanced by ALB within one region. We are currently experiencing poor performance for access from customers in non-regional countries. What can I do to improve performance?

* + Host your static files on S3.
  + Take advantage of Lightsail.
  + **Use CloudFront.**
  + Use ECS.

**Correct**

This question asks how to improve performance when delivering a website to users around the world. In this case, using CloudFront is effective. By using CloudFront, you can have website caches all over the world. Users will access the cache closest to them, which can improve performance. So option 3 is the correct answer. Option 1 is incorrect. S3 is a storage service tied to a region, and performance improvement cannot be expected for geographically distant users. Option 2 is incorrect. Lightsail is a cost-effective virtual private server that has everything you need to build an application or website. When building a website, you can deploy web applications with just a few clicks. This service is useful when you want to easily build a simple website, but it is not suitable for distributing websites around the world. Option 4 is incorrect. ECS is a container service. Changing an EC2 instance to ECS will not improve performance.

1. 10. Question

A web application accessible from the Internet utilizes a MySQL database running on an EC2 instance in a private subnet. Increasingly complex queries with multiple table joins are increasing the load on the database and degrading the performance of the application. The application team is looking into ways to improve performance. What suggestions can the solution architect give the application team to improve performance while scaling the database?

* + Cache query data in SQS.
  + Migrate your database to Athena.
  + **Migrate your database to Aurora MySQL.**
  + Implement DynamoDB Accelerator to cache data.
  + **Create read replicas to offload queries.**

**Incorrect**

Fully managed Aurora MySQL outperforms MySQL running on EC2 in terms of availability, performance, and scalability. For Aurora, you can easily scale read-only traffic by adding read replica instances. So it‘s best to migrate the database to Aurora MySQL and create a read replica. So option 3 and option 5 are correct. Option 1 is incorrect. SQS is a message queuing service that retrieves queued data asynchronously. Not suitable for caching query data. Option 2 is incorrect. Athena is a service that queries and processes data in S3. It is not a service that improves database performance. Option 4 is incorrect. DynamoDB Accelerator is a caching service for DynamoDB. DynamoDB is a NoSQL database, so it cannot handle complex queries involving multiple table joins.

1. 11. Question

Your company is developing a mobile application that manages large amounts of image data. Image data uploaded from a mobile terminal generates multiple thumbnails on EC2 and is stored in storage. Front EC2 is load balanced to multiple instances with ALB. Thumbnail files must be drawn simultaneously within a few seconds on a mobile device, but original image files are not drawn and are only downloaded from mobile devices. Which AWS service is cost-effective to store original image files?

* + EBS Volumes on General Purpose SSDs
  + EFS
  + **S3**
  + S3 Glacier

**Correct**

S3 is cost effective for storing large files like original image files that can be accessed by multiple EC2 instances. Compared to EBS, S3 has lower file read/write performance, so it is not suitable for drawing multiple thumbnails in a short time. There is no problem in that it is inferior. So option 3 is the correct answer. Option 1 is incorrect. EBS volumes meet the requirements for reading and writing thumbnail files, but general-purpose SSD type EBS volumes cannot be shared on multiple EC2 instances. Option 2 is incorrect. EFS is good for storing thumbnail images, but costs more than S3 for storing original image files. Option 4 is incorrect. S3 Glacier is not suitable in terms of usability, as files cannot be referenced directly and it takes several hours to retrieve files.

1. 12. Question

A startup company is building a web application. The frontend consists of static content and the application layer consists of microservices. User data must be in JSON format and accessible with low latency. Traffic to the application is normally not high, but it is expected that traffic will temporarily increase when new features are launched. Startup development teams want to minimize maintenance costs. Which solution is right for you?

* + Use S3 static site hosting for the front end and Elastic Beanstalk for the application layer. User data is stored in DynamoDB.
  + Use S3 static site hosting for the front end and EKS for the application layer. User data is stored in RDS.
  + **Use S3 static site hosting for the front end and Lambda for the application layer. User data is stored in DynamoDB.**
  + **Use S3 static site hosting for the front end and Lambda for the application layer. User data is stored in RDS.**

**Incorrect**

Store static content in S3 and enable website hosting. Since the application layer consists of microservices, EKS or Lambda are suitable. In addition, master data such as user data can be accessed with lower latency by using DynamoDB, which is a key-value store, than RDS, and it is possible to cope with temporary traffic increases at low cost. So option 3 is the correct answer. Option 1 is incorrect. Blastic Beanstalk is not the best configuration for microservices. In the case of Lambda, a serverless service, you can build a code execution environment in small units like microservices, and even if traffic increases temporarily, it will automatically scale, reducing operating costs. Responding to temporary traffic spikes in Blastic Beanstalk requires auto scaling to be set up and properly operated by the consumer, which is also suboptimal. Option 2 is incorrect. When storing in RDS, scaling up is necessary when traffic increases temporarily. Also, user data in JSON format works well with key-value stores, and DynamoDB has the lowest cost and low-latency access over RDS. Option 4 is incorrect. Similar to Option 2, DynamoDB meets the requirements at the lowest cost over RDS for the workload in question.

1. 13. Question

A developer is building a new online transaction processing (OLTP) application for a small, highly read-write intensive database. A single table in the database is continuously updated throughout the day, so developers want to ensure good performance in database access. Which EBS storage option is suitable for maintaining application performance?

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

**Correct**

Provisioned IOPS SSD is an EBS storage that is suitable for ensuring sufficient performance in online transaction processing and frequently accessing small size data while maintaining performance. So option 1 is the correct answer. Option 2 is incorrect. General Purpose SSDs are solid-state drive storage, but cannot scale to as high a performance as Provisioned IOPS SSDs. Option 3 is incorrect. Cold HDD is storage for throughput oriented and infrequently accessed data. It is not suitable for use as a storage that frequently accesses data. Option 4 is incorrect. Throughput-optimized HDDs are hard disks for frequently accessed processes that require high throughput. It is suitable for processing targeting big data.

1. 14. Question

A company is reviewing the number of EC2 instances provisioned in its Auto Scaling group. The Auto Scaling group currently utilizes 2 AZs with a minimum of 2 and a maximum of 6 instances. When I checked the CloudWatch metrics, I saw steady low CPU utilization. Reduce costs while maintaining application availability Which solution to optimize? (Select one)

* + Decrease the minimum number of instance launches to increase CPU utilization.
  + Decrease the maximum number of instance launches to increase CPU utilization.
  + **Change the metric in the Auto Scaling group‘s scaling policy to CPU utilization.**
  + Set a large instance type in the Auto Scaling group‘s launch configuration.

**Correct**

Steady low CPU utilization means that the scaling policy is increasing the number of instances before the CPU utilization increases. You can increase resource utilization by setting scaling policies based on CPU utilization to add instances only when CPU utilization rises to a certain level. So option 3 is the correct answer. Option 1 is incorrect. For this question, the minimum number of instance launches is 2. If you reduce the minimum number of instance launches, the minimum value will be 1, which will result in a single AZ configuration and availability will not be maintained. Option 2 is incorrect. By reducing the maximum number of instances that can be started, you can expect an increase in CPU utilization when the system is maximally scaled out. Option 4 is incorrect. Larger instance types result in even lower CPU utilization.

1. 15. Question

The system you are building on AWS requires data encryption to handle confidential data, and has the following management requirements for encryption keys. ?Managed as a single tenant ?Cryptographic module that satisfies FIPS 140-2 Level 3 Which is the best solution to meet the above requirements?

* + Manage encryption keys with KMS.
  + **Manage encryption keys with CloudHSM.**
  + Manage encryption keys on-premises.
  + **Manage encryption keys with KMS and audit with CloudTrail.**

**Incorrect**

It requires single tenant and cryptographic key management that meets FIPS 140-2 Level 3 requirements. The services that manage encryption keys are KMS and CloudHSM, but CloudHSM meets the requirements of the question, so option 2 is the correct answer. FIPS 140-2 is a US federal government standard for cryptographic modules. Security requirements are defined by level, KMS meets level 2 and CloudHSM meets level 3.

1. 16. Question

A company has a website that receives approximately 1,000 transactions of API requests daily from a mobile application, displaying tens of kB of content with an average response time of 50 ms. This system is currently hosted on a single m5.xlarge instance. What changes would you make to this system to achieve a cost-effective, highly available architecture?

* + Create an Auto Scaling group with a minimum of 1 and a maximum of 2 instances and use ALBs to distribute traffic.
  + **Recreate the API using Amazon API Gateway and use Lambda as the service backend.**
  + Create an Auto Scaling group with up to two instances and use ALBs to distribute traffic.
  + Recreate the API using Amazon API Gateway, using the new API and an existing EC2 instance as the backend.

**Correct**

In the case of the question, a website with simple processing and short processing time is implemented on the server side. In this case, switching to an implementation using Lambda is more cost-effective than implementing it on an EC2 instance because it is pay-as-you-go. Lambda runs in multiple AZs, ensuring high availability. So option 2 is the correct answer. Options 1 and 3 are incorrect. Using Auto Scaling to flexibly increase or decrease the number of EC2 instances is suitable for performing complex processing according to load, but the cost is higher than with Lambda. Option 4 is incorrect. Setting up Amazon API Gateway and integrating it with a backend EC2 instance doesn‘t cut costs.

1. 17. Question

A company needs to configure AWS Organizations to manage multiple AWS accounts for each business unit. A Solution Architect has granted the following Service Control Policy (SCP) to an Organization Unit (OU) to control the services consumed by member accounts. { “Version“: “2012-10-17“, “Statement“: { “Effect“: “Allow“, “Action“: [“ec2: \*“, “rds: \*“], “Resource“: “\*“ } } IAM users of member accounts under the OU were able to create EC2 instances, but not RDS instances. Which action is required to create an RDS instance?

* + **Set IAM policy to OU instead of SCP.**
  + Create an RDS instance using the root user of your AWS account.
  + **Set an IAM policy that allows IAM users to create RDS instances.**
  + Explicitly set RDS instance creation rights to the OU‘s SCP.

**Incorrect**

SCP has been granted access to RDS. Option 3 is the correct answer because the IAM user may not have the necessary permissions to create the RDS instance. Option 1 is incorrect. OUs cannot have IAM policies. Option 2 is incorrect. While it may be possible to create an RDS instance with the root user, it is not recommended as a best practice. Option 4 is incorrect. In SCP, it is possible to set the availability of each service, but it is not possible to set the availability of specific operations within the service.

1. 18. Question

A solution architect is designing an application that uses EBS volumes on EC2 running in the Tokyo region of AWS. As a disaster countermeasure, it is necessary to back up the EBS volume in another region and restore the EBS volume in another region when a disaster occurs. What is the most efficient way to meet this requirement?

* + Create an EBS snapshot directly from one region to another.
  + Move data to an S3 bucket and enable cross-region replication.
  + **Create an EBS snapshot and then copy it to the desired region.**
  + Use a script to copy data from the current EBS volume to the destination EBS volume.

**Correct**

When copying EBS volumes between the Tokyo region and another region, create an EBS snapshot. Then copy the snapshot from the Tokyo region to another region. So option 3 is the correct answer. Option 1 is incorrect. EBS volumes cannot be directly snapshotted across regions. Option 2 is incorrect. You can copy data to S3 and copy between regions with S3 inter-region replication, but you need to create a custom process to copy all the data in the EBS volume to S3. Option 4 is incorrect. Copying directly to an EBS volume in another region also requires a custom copy process, similar to Option 2.

1. 19. Question

You are responsible for building the infrastructure for a publicly available web service on AWS. I have already created 2 public and 2 private subnets on my VPC. Web applications are developed as microservices, so you will build multiple EC2s to place those resources. Depending on the URL, you will need to target different EC2 instances to route the requests. Which load balancer best practice meets these requirements?

* + Build NLB in public subnet. Build multiple EC2s in private subnets. Distributes requests from NLB to EC2 according to the URL.
  + Build NLB in public subnet. Build multiple EC2s in public subnets. Distribute requests from NLB to EC2 according to the URL.
  + **Build ALB in public subnet. Build EC2 with private subnet. Distribute requests from ALB to EC2 according to the URL.**
  + Build an ALB in a private subnet. Build EC2 with private subnet. Distribute requests from ALB to EC2 according to the URL.

**Correct**

Since this is a publicly exposed web service, we need to allow external access. Also, access from the outside must be accepted by the load balancer placed in the public subnet. ALB can distribute requests according to URLs by setting listener rules. On the other hand, NLB cannot distribute requests to targets according to the URL only by setting the load balancer. Therefore, Option 3, which uses ALB in a public subnet and distributes requests to EC2 in a private subnet as a target, is the correct answer. Option 1 is incorrect. Since MB settings alone cannot respond to URLs or distribute quests, it is necessary to create a separate mechanism such as a reverse proxy, which is not the best practice compared to Option 3. Option 2 is incorrect. Deploying EC2 in a public subnet as a server for the Tb application is easy to attack from the Internet and is not desirable from a security point of view. Also, as with A, NLB alone cannot distribute requests to targets according to URLs. Option 4 is incorrect. If you configure your ALB in a private subnet, you will not be able to accept public access.

1. 20. Question

A company is building a data lake using S3. Data is required to be encrypted at rest because it contains sensitive information. Additionally, encryption must utilize encryption keys provided by the security team. Which solution meets these requirements? (Choose 2)

* + configure server-side encryption for S3 (SSE-S3);
  + **Configure encryption with your encryption key (SSE-C).**
  + **Configure encryption with a customer master key (CMK) stored in KMS (SSE-KMS).**
  + S3 does not support encryption with user encryption keys.
  + Upload the encryption key to the bucket and enable encryption for the bucket.

**Incorrect**

SSE-C and SSE-KMS are two ways to encrypt objects stored in S3 using existing encryption keys. So option 2 and option 3 are correct. SSE-C uses a user-managed encryption key to enclose and encrypt the key and data when uploading to S3. SSE-KMS, on the other hand, is the technique of importing encryption keys into KMS and configuring S3 encryption with the imported encryption keys. Option 1 is incorrect. SSE-S3 uses AWS-managed encryption keys to encrypt data at rest. The encryption key provided by the security team is not available and does not meet the requirements. Option 4 is incorrect. S3 has encryption capabilities with user-managed encryption keys. Option 5 is incorrect. You do not need to upload encryption keys to your S3 bucket to configure S3 encryption.

1. 21. Question

A company has been storing analytical data in DynamoDB for the past few years. The company asked its solution architects to come up with a solution that would allow users to access this data using an API. Set up Amazon API Gateway for your API and get data from DynamoDB on the backend. The API references a few data items (hundreds of bytes) from the database. Application usage can be bursty with traffic for a few seconds, although there are periods of light load. Which AWS service would you use for the backend of Amazon API Gateway as a cost-effective solution for dealing with sudden high loads?

* + ECS
  + **Lambda**
  + Elastic Beanstalk
  + EC2 Auto Scaling

**Correct**

Lambda is a service that can respond instantly even if the load suddenly increases. Lambda has a maximum payload size limit of 6MB, but the data size obtained by this API is several hundred bytes, so it doesn‘t hit the limit. So option 2 is the correct answer. Option 1 is incorrect. ECS is a container management service. Although it can handle sudden spikes, it is less cost-effective than pay-as-you-go Lambda. Options 3 and 4 are incorrect. Elastic Beanstalk and EC2 Auto Scaling are not suitable for scales that require instant responsiveness, as scaling out requires lead time for instance launch.

1. 22. Question

Your company operates a service that provides illustrations. Illustrations are currently stored in S3 Standard and access is random. As a solution architect, you have been asked to keep storage costs down. Which AWS services are effective in reducing costs?

* + EBS
  + S3 Glacier
  + EFS VU
  + **S3 Intelligent-Tiering**

**Correct**

S3 Intelligent-Tiering is an S3 storage class that automatically moves files to the appropriate storage class. Although there is a monthly monitoring fee, you can analyze file access patterns and move files to the most cost-effective class. In this question, all illustration files do not have a common access pattern and are accessed randomly. Therefore, storing files in S3 Intelligent-Tiering is the most efficient and cost effective method. So option 4 is the correct answer. Option 1 is incorrect. EBS is a block storage service and has higher storage costs than S3 Standard. Option 2 is incorrect. With S3 Glacier, file storage costs are lower, but file access takes longer. Option 3 is incorrect. EFS is a file storage service and has higher storage costs than S3 Standard.

1. 23. Question

A developer wants to build an online approval system for internal use. We expect the approval process to take up to two days. Serverless solutions should be designed to reduce system maintenance effort as much as possible. Which processing method meets your requirements?

* + **Use Lambda and Step Functions.**
  + **Put all the processing in a single Lambda function.**
  + Using ECS ??on EC2.
  + Use Lambda and Amazon API Gateway.

**Incorrect**

Step Functions can set up an approval process for your workflow. Standard workflows can run for up to a year, so it‘s okay if the approval process takes up to two days. So option 1 is the correct answer. Option 2 is incorrect. Lambda‘s maximum timeout value is 15 minutes, so processing with Lambda alone is not suitable for cases with long waiting times like this question. Option 3 is incorrect. ECS allows you to run applications in containers, but they are launched on EC2, which requires EC2 maintenance. Option 4 is incorrect. Amazon API Gateway has a maximum timeout value of 29 seconds, so it is not suitable for long-latency processing.

1. 24. Question

I‘m building an application that runs on EC2 instances deployed in multiple AZs. Security policies dictate encryption of data in EC2 and backup data. Also, since the project budget is limited, we would like to achieve encryption at the lowest possible cost. Which is the best solution to meet these requirements?

* + Configure AWS managed customer master key (CMK) EBS encryption. Encrypt the snapshot in the backup job after taking the EBS snapshot.
  + Encrypt the data in the application and write it to EC2.
  + **EBS and EBS snapshots are encrypted by default.**
  + **Create a user-managed CMK in KMS and enable EBS encryption on the created CMK. EBS snapshots are automatically encrypted.**

**Incorrect**

To configure EBS encryption, you must enable encryption while configuring EC2 (EBS). When you enable EBS encryption, your EBS snapshots are automatically encrypted as well, helping you meet your backup data encryption requirements. So option 4 is the correct answer. For EBS encryption, you can specify an AWS managed CMK or a user managed CMK created with KMS as the encryption key. Option 1 is incorrect. By enabling EBS encryption, EBS snapshots are automatically encrypted as well, so there is no need to encrypt them in your backup jobs. Option 2 is incorrect. Application encryption can meet the requirements, but it requires explicit processing in the application and is not cost-optimal compared to EBS encryption which automatically encrypts. Option 3 is incorrect. EBS is not encrypted by default.

1. 25. Question

Our call center application runs on EC2 and consists of an Auto Scaling group. Automatically scale resources according to load. Operators work from 9:00 am to 5:00 pm, and the system is very slow, especially between 9:00 am and about 15 minutes each morning. Most of the call center staff are scheduled to start work at 9:00 a.m. Before 9:00 a.m., they log into the application and prepare for work. How can a solution architect efficiently ensure that the right resources are available to handle the heavy load each morning?

* + **Create an Auto Scaling scheduled action to scale out the required resources at 8:30 am every morning.**
  + Use Reserved Instances to ensure your system reserves adequate capacity for scale-up events.
  + To guarantee available resources, take advantage of Spot Instances and reserve the instances you need before 9am.
  + Start an EC2 instance that is larger than the one currently running so that it can handle high loads.

**Correct**

The question is what kind of settings should be made in order to secure the necessary resources according to the load. As in the question, if you know that the load will be high at 9 am every morning and the high load will continue for about 15 minutes, scale out early and secure sufficient resources at 9 am. must be So option 1 is the correct answer. Option 2 is incorrect. A Reserved Instance is a service that allows you to reduce your EC2 usage costs when using the same instance for a long period of time. The longer you use the service, the Increase cost efficiency. Option 3 is incorrect. Spot Instances allow you to launch instances at a low cost, but they are not guaranteed to keep running for 15 minutes, so your instances may be interrupted at unintended times. Option 4 is incorrect. The operation of scaling up, launching a large instance, and scaling it down after 15 minutes is time consuming and not an efficient operation that flexibly increases or decreases resources.

1. 26. Question

Solution architects are looking at ways to encrypt RDS instances during launch. Which method is the most appropriate?

* + **Take a snapshot of your DB instance. Copy the snapshot with the Enable Encryption option selected. Restore a DB instance from a copied snapshot.**
  + Take a snapshot of your DB instance. Restore a DB instance from a snapshot with the “Encryption Enabled“ option selected.
  + **Take a snapshot of your DB instance with the Enable encryption option selected. Restore a DB instance from a snapshot.**
  + Stop the DB instance. Launch a DB instance with the Encryption Enabled option selected.

**Incorrect**

It is not possible to enable the encryption feature on a running RDS instance, but it is possible to encrypt the copy of the snapshot taken. Select the Enable Encryption option when copying the snapshot. This allows you to restore the encrypted instance from the copied snapshot. So option 1 is the correct answer.

1. 27. Question

Your company is building a static content-centric website. The website will utilize a custom domain name and access to the website should be low latency. We also want to operate serverless to reduce the cost of building and operating servers. Which AWS service is right for me?

* + ELBs
  + ECS Fargate
  + EBS
  + **CloudFront**

**Correct**

For static content-centric websites, you can build a configuration that distributes web content serverless and with low latency by placing static content in S3 and distributing it with CloudFront. CloudFront is a CDN service that delivers content, and can be used at a relatively low cost while caching large files. So option 4 is the correct answer. Option 1 is incorrect. ELB is a load balancer and is usually placed in front of EC2 or ECS and used for load balancing purposes. Option 2 is incorrect. Since ECS requires building and operating a web server, it is inappropriate from a serverless perspective. Option 3 is incorrect. EBS is block storage attached to an EC2 instance. Not suitable from a serverless perspective as it requires EC2.

1. 28. Question

A company backs up approximately 50TB of data to tape daily and stores application data offsite. Backups must be retained for 7 years for compliance purposes. We rarely have access to backup files, and if we need to restore a backup, we typically give 5 business days‘ notice. The company is currently exploring cloud-based capabilities to reduce the storage costs and operational burden of tape management, and wants to minimize the disruption of migrating from tape backup to the cloud. Which storage solution is the most cost effective?

* + Integrate backups directly with S3 Glacier using Snowball Edge.
  + Manually copy the backup data to S3, create a lifecycle policy, and move the data to S3 Glacier.
  + **Back up to S3 Glacier Deep Archive using Storage Gateway‘s tape gateway.**
  + **Backup to S3 using Storage Gateway‘s Volume Gateway and create a lifecycle policy to move backups to S3 Glacier.**

**Incorrect**

When migrating to AWS, it is a requirement to transfer large amounts of data to AWS every day and retain that data for 7 years. Here, since high cost-effectiveness is required and there is a grace period of 5 business days for data retrieval, it is assumed that S3 Glacier Deep Archive will be used. Storage Gateway‘s Tape Gateway is also the most efficient implementation as it provides direct connectivity to S3 Glacier Deep Archive. So option 3 is the correct answer. Option 1 is incorrect. Snowball Edge cannot connect directly to S3 Glacier. Option 2 is incorrect. Higher migration costs due to the need for manual backups. Option 4 is incorrect. Option 3, which stores data directly in S3 Glacier Deep Archive, is more cost-effective than placing it temporarily in S3.

1. 29. Question

Your application is running on EC2 in multiple regions, and the EC2 instance loads sensitive configuration from an S3 bucket on startup and uses DynamoDB as the database. The security team has advised you to use private networks instead of using public endpoints to access AWS services for better security. Which of the following is a valid change to address this issue? (Choose 2)

* + **Create a gateway VPC endpoint for S3. Create an interface VPC endpoint to DynamoDB.**
  + **Create an interface VPC endpoint for S3. Create a gateway VPC endpoint to DynamoDB.**
  + **Create interface VPC endpoints for S3, DynamoDB.**
  + Create a security group and set rules to allow communication to S3 and DynamoDB.
  + **Modify your route table to route traffic to DynamoDB to your VPC endpoint.**

**Incorrect**

This question asks you to configure private communication from within your VPC to S3 and DynamoDB using VPC endpoints. There are two types of VPC endpoints: gateway type and interface type. S3 is a service that supports both interface type and gateway type, and DynamoDB is a service that supports only gateway type, so option 2 is the correct answer. Also, in order to use a gateway type VPC endpoint, it is necessary to change the route table of the subnet and route the communication to DynamoDB to the VPC endpoint, so option 5 is also correct.

1. 30. Question

A company wants to migrate its on-premises Oracle database to RDS for Oracle in the Tokyo region. The Chief Technology Officer (CTO) wants a disaster recovery plan to keep the database available in the Singapore region in case the database becomes unavailable in the Tokyo region. Recovery should have an RTO (Recovery Time Objective) of 3 hours and an RPO (Recovery Point Objective) of 4 hours or less. How should we meet these requirements while minimizing downtime?

* + Specify VPCs that exist in the Tokyo region and Singapore region, and provision RDS with multi-master cluster enabled.
  + Create automated snapshots of RDS and copy to Singapore region every 4 hours. During recovery, provision RDS in the Singapore region using the latest snapshot.
  + **Create an RDS read replica in the Singapore region. During recovery, promote the read replica in the Singapore region to master.**
  + **Enable RDS multi-region deployment and provision a standby instance in the Singapore region. Upon recovery, the standby instance in the Singapore region automatically promotes to master.**

**Incorrect**

You can achieve disaster recovery by creating cross-region read replicas and promoting them to masters in the event of a failure. So option 3 is the correct answer. Option 1 is incorrect. Multi-master clusters can be used within the same region for Aurora, but not for RDS for Oracle. Option 2 is incorrect. Recovery is possible by copying a snapshot and using it. However, restoring from a snapshot will result in longer downtime compared to Option 3. Option 4 is incorrect. RDS has a setting for multi-AZ deployments, but not for provisioning standby instances in multi-region deployments.

1. 31. Question

Your company is trying to run an in-house system on EC2. The system has peak hours each day and requires up to 6,000 IOPS during peak hours. As a solution architect, you need to choose storage that performs well at peak times and is cost-effective. Which storage type is best?

* + **EBS General Purpose SSD (gp2)**
  + EBS cold HDD (sc1)
  + **EBS Provisioned IOPS SSD (iO1)**
  + EBS Throughput Optimized HDD (st1)

**Incorrect**

EBS has various storage types, so you need to choose the right type according to your system requirements. For this question, a maximum of 6,000 IOPS is required and HDD types sc1 and st1 cannot meet the requirement. Both gp2 and io1, which are SSD types, can meet your requirements, so you should choose gp2, which is cheaper. So option 1 is the correct answer. Option 2 is incorrect. The EBS cold HDD (sc1) does not meet the requirements of the question as it has a max IOPS of 250. Option 3 is incorrect. EBS Provisioned IOPS SSD (io1) meets the maximum IOPS requirement, but has a higher usage fee compared to EBS General Purpose SSD (gp2). Option 4 is incorrect. The EBS Throughput Optimized HDD (st1) does not meet the requirements of the question as it has a maximum IOPS of 500.

1. 32. Question

You are using CloudFront to develop a web application service for Japan. Which of the following methods restricts access sources to distributed content only within Japan?

* + Add GeoIP in Japan in the security group.
  + Deny all GeoIPs outside of Japan in your network ACL.
  + Enable the geographic distribution feature in your S3 bucket policy and add Japan to your whitelist.
  + **Enable CloudFront‘s geographic distribution feature and add Japan to the whitelist.**

**Unattempted**

CloudFront‘s geographic distribution feature allows you to restrict access on a country-by-country basis. You can select the Allow or Deny action by specifying the geographic region of the originating GeoIP of the request. So option 4 is the correct answer. Options 1 and 2 are incorrect. Neither security groups nor network ACLs are methods of restricting access to delivered content. Option 3 is incorrect. There is no geographic distribution feature in S3 bucket policies, and S3 is independent of how access to distributed content is restricted.

1. 33. Question

You are designing a web architecture for a game application consisting of an application server and a database server. In the near future, we will be launching a new service for a popular application, and we anticipate a significant increase in access as a result. Solution architects must prevent the RDS for MySQL database from becoming a bottleneck due to frequently accessed queries. What services or features should the solution architect add?

* + **Take advantage of the Multi-AZ feature of the RDS for MySQL database.**
  + Place CLB in front of the web application layer to increase the number of web application servers and distribute the transaction load.
  + Place SQS in front of RDS for MySQL database to process transactions asynchronously.
  + **Place ElastiCache in front of your RDS for MySQL database to cache some data.**

**Incorrect**

For this question, storing some of the data in the RDS for MySQL database in ElastiCache is an effective means of distributing processing transactions and reducing RDS for MySQL processing. So option 4 is the correct answer. Option 1 is incorrect. Multi-AZ machine is a machine to achieve high availability of database. In the case of Otome, even with a multi-AZ configuration, transactions from the application server are processed by the master‘s RDS, so the amount of RDS transactions does not change. Option 2 is incorrect. When the load of the web application layer is distributed, the load per application server is reduced, but the amount of transactions to RDS remains the same. Option 3 is incorrect. Deploying SQS queues transactions and allows you to process all transactions asynchronously. Since it waits in the queue, the load on RDS is temporarily reduced, but as a result, the number of requests to RDS does not change, and it takes time to process the entire transaction.

1. 34. Question

You work as a solution architect at a startup company. The startup offers payment services and uses third-party payment services to process payments. The system is running on a group of EC2 servers, and ELB distributes to the servers. Also, the payment service requires connection over the internet and allows up to 5 IP addresses at a time. Which is the most secure solution that meets these requirements?

* + **Place ELB in public subnet and EC2 in private subnet. Place a NAT gateway in the public subnet and change the private subnet‘s route table to set internet access from EC2 via the NAT gateway.**
  + Place ELB and EC2 in public subnet. Define an IP address that can connect to the payment service in the security group and attach it to EC2.
  + Place ELB in public subnet and EC2 in private subnet. Place the customer gateway in a public subnet and modify the private subnet‘s route table to allow Internet access from EC2 through the customer gateway.
  + Place ELB and EC2 in public subnet. Define network ACLs that allow IP addresses to communicate with payment services and block all other internet-bound traffic.

**Correct**

Due to the limited number of IP addresses that can connect to payment services, we use NAT gateways to fix public IP addresses. This removes the limit on the number of EC2 servers. Also, placing EC2 servers in a public subnet is not a recommended configuration for security, so option 1 is the correct answer.

1. 35. Question

Your company uses AWS to build a system in your project AWS account. The system should be built according to the guidelines of the operations team. The operation guidelines stipulate that logs should be aggregated in a separate AWS account for the operation team, and the operation team may view the AWS account in which the system was built when an error is detected from the logs. How to grant access to the operations team according to the principle of least privilege? (Select one)

* + Create new IAM users for operations team members who need access.
  + **Launch EC2 and apply necessary permissions to EC2 using IAM roles. Connect with the AWS account for the operations team via VPC peering. The operation team can access with this EC2SSH and view the necessary information using AWS CLI.**
  + **Add the operations team account to the trust policy using an IAM role.**
  + From the AWS account for the operation team, apply for permission to the AWS account for the project. Access will be granted once the application is approved.

**Incorrect**

To allow access from another AWS account, we recommend setting up cross-account access using an IAM role. Set permission policies for IAM roles according to the principle of least privilege. Use of elevated permissions is restricted to only when necessary for specific tasks. Using IAM roles helps prevent accidental changes to sensitive environments. For cross-account access, use an IAM role trust policy to allow AssumeRole from specific AWS accounts. You control which AWS accounts have access by specifying the external ID as a Condition in your trust policy. From the above, option 3 is the correct answer. Options 1 and 2 are incorrect. Inappropriate because there is another way to grant permissions to users in different AWS accounts without using cross-account permissions. Option 4 is incorrect. Inappropriate because it does not provide a function to request access permission.

1. 36. Question

A developer is designing a solution for a static Single Page Application (SPA) that is used all over the world. Solutions must have low operating costs and low latency. Which AWS services should developers combine? (Choose 2)

* + RDS
  + Auto Scaling
  + **S3**
  + NLBMore
  + **CloudFront**

**Incorrect**

With S3 static website hosting, you can implement a static SPA at a low cost. Also, by using CloudFront, it is possible to provide content around the world with low latency. Therefore, options 3 and 5 are the correct answer, as they can be combined to provide a low-cost, low-latency static application. Option 1 is incorrect. Since the solution is for static applications, RDS is not required. Option 2 is incorrect. Using Auto Scaling groups to host static applications has higher operational costs than using S3. Option 4 is incorrect. NLB is unsuitable as it can only be combined with Auto Scaling Groups among the options, resulting in high operational costs.

1. 37. Question

Your accounting application runs on-premises and uses MySQL as its database. The business department reported that there were times when performance degraded, and analysis revealed that it occurred when users were performing reporting tasks during working hours. You are looking to improve performance and are considering moving to AWS. Which solution is the most cost-effective from a build and operations perspective? (Select one)

* + Create a database on an EC2 instance. Make sure that the computing resources such as the number of CPU cores have specifications equal to or higher than the existing database.
  + Build DynamoDB and import data into the table. Refurbish the application to use DynamoDB for reporting.
  + **Deploy Aurora MySQL in Multi-AZ. Modify your application to use the cluster‘s backup instance as the reporting endpoint.**
  + **Deploy Aurora MySQL in Multi-AZ with multiple read replicas. Modify your application to use the read replica endpoint for reporting.**

**Incorrect**

In this case, reporting in real time is causing performance issues. For this reason, it is important to separate the reporting process. By using a read replica, you can reduce the load on the master node and improve the write performance.In addition, the use of a read replica can be easily executed from the AWS console screen, and the man-hours for construction work can be reduced. increase. So option 4 is the correct answer. Option 1 is incorrect. Reporting process is not separated and it is unclear if it will improve performance am. Also, running a database on EC2 increases operational costs compared to using Aurora MySQL. Option 2 is incorrect. Since our existing applications use MySQL, we need to make use of a relational database. Using a key-value type NoSQL database like DynamoDB incurs data migration, which incurs costs. Option 3 is incorrect. In a Multi-AZ environment, a standby instance can be used for read-only processing. is inappropriate because it cannot be used.

1. 38. Question

I have a web service configured on an ALB and an EC2 instance. Instances run in an EC2 Auto Scaling group that spans two AZs. A minimum of 4 instances is required for stable operation of this system. How do you meet the required service level agreements (SLAs) while containing costs in the event of an AZ failure? (Select one)

* + **Modify the Auto Scaling group to run 6 EC2 instances in 3 AZs.**
  + Add a target tracking scaling policy with a short cooldown period.
  + Change the Auto Scaling group‘s launch configuration to use a larger instance type.
  + Modify your Auto Scaling group to run 8 EC2 instances in 2 AZs.

**Correct**

With 6 EC2 Auto Scaling groups (3AZ x 2), even if one AZ fails, it will be possible to operate with 4 units. So option 4 is the correct answer. Option 2 is incorrect. A target tracking scaling policy uses a target A service that minimizes sudden fluctuations in Auto Scaling by keeping it close to its value. Adding a target tracking scaling policy with a short cooldown period does not address AZ failures. Option 3 is incorrect. Scaling up EC2 instance types improves performance, but does not provide high availability to AZ failures. Option 4 is incorrect. By setting the EC2 Auto Scaling group to 8 units (2AZ x 4 units), it is possible to operate with 4 units even if one AZ fails, but the cost is higher than the option 1 method. increase.

1. 39. Question

A service that your team is responsible for provides monthly invoices to customers in PDF format. The current month‘s issued invoices are frequently accessed by the accounting team, but historical invoices are accessed infrequently and only when a customer requests a reissue. Invoices must be provided within 8 hours for this reissue request. Recently, the number of customers has increased and storage costs have risen, so the team leader is motivated to propose a cost-conscious solution. I requested you to Which is the best solution? (Select one)

* + **Store the current month‘s invoices in S3 and move past invoices to S3 Glacier using a lifecycle policy. If there is a request for reissue, it is taken out using the standard option.**
  + Store the current month‘s invoices in S3 and move past invoices to S3 Glacier Deep Archive using a lifecycle policy. If there is a request for reissue, take it out using the quick option.
  + Store the current month‘s invoices in S3 and move past invoices to S3 Glacier using a lifecycle policy. If there is a request for reissue, take it out using the quick option.
  + Store the current month‘s invoices in S3 and move past invoices to S3 Glacier Deep Archive using a lifecycle policy. If there is a request for reissuance, it is taken out using the standard option.

**Correct**

Both S3 Glacier and S3 Glacier Deep Archive can store files at a low cost, but accessing files requires time and money to retrieve them. Pick-up times vary by option, with shorter pick-up times costing more. The problem statement states that past invoices are accessed less frequently than current month invoices and should be reissued within 8 hours.In this case, it is better to save files in S3 Glacier than S3. Cost effective. Also, when choosing between S3 Glacier and S3 Glacier Deep Archive, you must choose S3Glacier to meet the “within 8 hours“ condition. When doing so, consider the cost and choose the standard option of S3 Glacier. So option 1 is the correct answer. Option 2 is incorrect. S3 Glacier Deep Archive does not offer an expedited option. Option 3 is incorrect. S3 Glacier‘s expedited option has a retrieval time of 1-5 minutes. However, even with the standard option, you can take it out in 3 to 5 hours, so you can reduce the cost by choosing the standard option this time. Option 4 is incorrect. Standard option retrieval time for S3 Glacier Deep Archive is less than 12 hours. Therefore, this option is incorrect as it may not be possible to retrieve it within 8 hours.

1. 40. Question

Access S3 from an EC2 instance that exists within a VPC. I want to allow access from EC2 in the public subnet to read only, and want to allow access from EC2 in the private subnet to read as well as update. Access from EC2 to S3 within the VPC is via the gateway VPC endpoint. How can I achieve this? (Select one)

* + Use the aws: SourceIp condition in your bucket policy to allow updates from private subnets and read-only access from public subnets.
  + From the public subnet, set the route table to connect to S3 via the Internet without going through the VPC endpoint.
  + **Create two VPC endpoints, one for read-only and one for updates, and separate the VPC endpoints used in each subnet. Set the policies for each endpoint to allow S3 read actions for read-only endpoints, and allow S3 read and update actions for update endpoints.**
  + Add a rule to allow outbound traffic to the created VPC endpoint to the security group of the EC2 instance in the private subnet.

**Correct**

You can set access restrictions to specific S3 buckets in endpoint policies. You can also apply different permission settings by dividing the traversing endpoints by subnet. So option 3 is the correct answer.

1. 41. Question

A company operates an application server and a database server on-premises. Since the database server stores the data that is the core of business, it is necessary to prepare for quick recovery. You are currently choosing a storage solution for your backups. The requirements for backup storage are to minimize construction and operation costs and to provide instant access to backed up data. Which is the best solution to meet these requirements? (Select one)

* + **Deploy Storage Gateway File Gateway on-premises and transfer files to an S3 bucket.**
  + Mount EFS on-premises to store database backup files.
  + Get a database VM and periodically transfer it to an S3 bucket using the AWS CLI.
  + Back up the database to a Snowball device and use lifecycle rules to move the data to S3 Glacier Deep Archive.

**Correct**

By using the file gateway of Storage Gateway, it becomes possible to acquire backups to an S3 bucket. File sharing setup with SMB or NFS protocols is required, but because the gateway service is a managed service, initial setup and operational costs can be kept to a minimum. In addition, the backup data is stored in an S3 bucket, which satisfies the requirement of immediate access. So option 1 is the correct answer. is correct. Option 2 is incorrect. EFS can be mounted on multiple EC2 to share files, but it cannot be used by mounting on-premises. Option 3 is incorrect. Getting a VM and transferring it to an S3 bucket requires AWS CLI scripting, which increases the cost of building and operating compared to the Option 1 solution. Option 4 is incorrect. Snowball device is a service that backs up on-premises data to an external physical device and migrates it to AWS. However, there is a lead time for migration. Also, storing data in S3 Glacier Deep Archive takes time to retrieve.

1. 42. Question

Media companies operate on-premises systems that hold streaming data such as historical footage. This company is considering system migration from on-premises to AWS. The system uses temporary space for media content playback. Temporary space can store more than 5TB of data for several days and requires high performance and scalable storage in terms of I/O. Media content must retain data for the past year, and the amount of data is over 200TE. Also, stored content must always be accessible. Archive media content older than one year. Archived content is rarely accessed. Which set of services meets these requirements and is cost effective?

* + General purpose SSD EBS for temporary space, S3 for content storage, S3 for archive
  + **Use instance store for temporary space, S3 for content storage, and S3 Glacier for archive**
  + Use EBS with Provisioned IOPS for temporary space, EFS for content storage, and S3 Glacier for archiving
  + **Use EBS with Provisioned IOPS for temporary space, S3 for content storage, and S3 Glacier for archiving**

**Incorrect**

For this question, select a combination of storage solutions that meet your requirements for processing and storing media content and that is cost effective. There are three requirements for storage: ?The storage used as the temporary area must be able to store data for several days, have high-performance I/O, and be expandable. ?The storage that stores content within the past year must be large-capacity and accessible at all times. ?The storage that stores content older than one year is rarely accessed, but it is possible to archive large amounts of data. EBS with Provisioned IOPS for temporary space, S3 for content storage, and S3 Glacier for archiving are the best and cost-effective way to meet these requirements. So option 4 is the correct answer. Option 1 is incorrect. Using EBS with General Purpose SSD for temporary space is cheaper than EBS with Provisioned IOPS, but with a maximum IOPS of 16,000, Provisioned IOPS is a better choice if you want sustained IOPS performance. . Also, archived media content is accessed infrequently, so S3 Glacier is sufficient for archiving. Additionally, when it comes to content storage, using S3 is more expensive than S3 Glacier. Option 2 is incorrect. Instance store is used for temporary area. Instance store is EC2 volatile block storage. It is a higher IOPS storage than EBS and is suitable for storing caches and temporary content processing, but there is no persistence like EBS, so you may lose stored data. Option 3 is incorrect. When it comes to content storage, S3 can also meet your requirements. Using EFS instead of S3 provides better I/O performance than S3, but at a higher cost.

1. 43. Question

A company uses a large number of EC2s to perform batch processing with highly variable amounts of data. Batch processing is stateless and can be started and stopped at any time without affecting the system. This process typically takes 60 minutes. As a solution architect, you are being asked to design cost-effective and scalable solutions. What kind of solution do you propose?

* + **spot instance**
  + Reserved Instance
  + On-demand instance
  + **Lambda**

**Incorrect**

Spot instances and Lambda are good candidates, as batch processing is configured to be stateless and processing can be interrupted at any time. On the other hand, Lambda is a more cost-effective service than EC2 because you only pay for the amount of time that processing is running, not the waiting time for processing. Next, looking at the processing time, the question says “60 minutes“. This is longer than Lambda‘s timeout limit of 15 minutes, so it‘s not suitable for Lambda. So Spot Instances are the correct answer. Option 2 is incorrect. The case of the question is a batch process with large fluctuations in the amount of data, so it is a workload that makes it difficult to predict the capacity. Also, with Reserved Instances, it is necessary to commit to use for 1 or 3 years, and regular startup is a prerequisite for usage fees, so it is suitable for batch processing that takes 60 minutes. Is not … Option 3 is incorrect. On-Demand Instances are a regular price purchase option and are not as cost effective as Spot or Reserved Instances. Option 4 is incorrect. Lambda has a maximum uptime of 15 minutes, so it‘s not suitable for batch processing that takes 60 minutes to process.

1. 44. Question

You want to share the quotes you have created with your customers for a limited time, so you are considering file sharing via a signed URL. I created a signed URL for the file I uploaded on S3 and accessed it from the link, but I was unable to download the file. Which are the possible reasons?

* + Because you didn‘t create an IAM user for downloads.
  + **Because you didn‘t grant public-read to the bucket where you put the file.**
  + **Because the signed URL had expired.**
  + Because the user who created the signed URL was not the owner of the object on S3.

**Incorrect**

By process of elimination, option 1 is incorrect. Because you don‘t need an IAM user to access the object if you create a signed URL. You can grant someone a time-bound permission to access an object. Anyone who receives the signed URL will be able to access the object. Therefore, it is an inappropriate reason why the file cannot be downloaded. Option 2 is also incorrect. An object or bucket need not be public-read as long as it is private. Option 4 is also incorrect. Anyone with valid security credentials can create a signed URL. However, for successful access, the signed URL must be created by someone with permissions for the action you are trying to perform on the signed URL. In this case, the user creating the URL need not be the owner of the object, which is inappropriate. Based on the above, the most likely reason why the file could not be downloaded is option 3, “The signed URL has expired.“

1. 45. Question

A network engineer created two VPCs, named VPC1 and VPC2. I have EC2 running in each VPC and I need to access EC2 in VPC2 from EC2 in VPC1. Since applications exchange large amounts of data across EC2 across VPCs, communication between VPCs must have no single point of failure, have sufficient bandwidth, and be secure. Which solution is right to meet these requirements?

* + Configure Direct Connect on VPC1 and VPC2.
  + **Configure Transit Gateways in VPC1 and VPC2.**
  + Place a NAT gateway in VPC1 and direct EC2 communication to the NAT gateway.
  + **Configure a gateway VPC endpoint for EC2 running in VPC2 and configure routing from VPC1.**

**Incorrect**

It‘s a matter of choosing how to communicate between different VPCs. Use Transit Gateway for secure and highly available communication across VPCs. Transit Gateway has no single point of failure or bandwidth bottleneck and can be managed in one place even if the number of connected VPCs increases. So option 2 is the correct answer. Connectivity between VPCs is also possible with VPC peering. But VPC peering is only valid between two VPCs. As the number of connections between VPCs increases, each VPC will create a peering, creating a mesh state. Transit Gate can aggregate and manage routing information between VPCs. Option 1 is incorrect. Direct Connect is a service that connects the on-premises environment and AWS with a dedicated line. It does not connect between VPCs within AWS. Option 3 is incorrect. A NAT gateway is a service used when communicating from a private subnet within AWS to the Internet. It does not connect between VPCs. Option 4 is incorrect. Gateway VPC endpoint allows you to connect to AWS without going through the Internet You can use supported AWS services through Network Meat. However, the only AWS services that gateway VPC endpoints support are S3 and DynamoDB.

1. 46. Question

I have an application running on EC2, deployed in development and production environments. The development environment is used only during business days, while the production environment must be serviced 24/7. You, as an administrator, have been told to reduce your EC2 usage fees, and your development environment wants to prioritize cost over availability. Which is the most cost effective solution?

* + **Use Spot Instances for development and Reserved Instances for production.**
  + Use Reserved Instances for development and Spot Instances for production.
  + Use On-Demand Instances for development and Spot Instances for production.
  + **Use On-Demand Instances for development environments and Reserved Instances for production environments.**

**Incorrect**

The development environment is used only during business days, and Spot Instances are suitable because cost is prioritized over availability. On the other hand, the production environment is running 24 hours a day, 365 days a year, so Reserved Instances are suitable. So option 1 is the correct answer. Option 2 is incorrect. Since the development environment is only used on business days, Reserved Instances incur unnecessary costs for non-business days. Also, if you use spot instances for your production environment. Instances may be forcibly stopped by AWS, reducing availability. Options 3 and 4 are incorrect. On-Demand Instances are not a more cost-effective pricing model than Reserved Instances or Spot Instances. Development environments are required to prioritize cost over availability, so Spot Instances with lower prices are suitable.

1. 47. Question

A company operates a web service that delivers news content. The application runs on an EC2 instance behind the ALB. The instances run in an EC2 Auto Scaling group across multiple AZs and the database uses Aurora. Recently, there has been an increase in access to web services. Which AWS services are right for scalability and availability? (Choose 2)

* + AWS Shield
  + Direct Connect
  + **Aurora replica**
  + **CloudFront**
  + **AWS Global Accelerator**

**Incorrect**

The application at issue in this case is running on EC2 instances across multiple AZs (Availability Zones). In such cases, Aurora replication allows you to have up to 15 Aurora Replicas spread across AZs within a single AWS Region. This makes the database tier highly available. Also, by placing CloudFront in front of the ALB (Application Load Balancer), it is possible to distribute the content distribution load even when access to the application increases. So option 3 and option 4 are correct. Option 1 is incorrect. AwS Shield is a service that protects your applications from DDoS attacks. Option 2 is incorrect. Direct Connect is a service for connecting the on-premises internal network environment and the AWS environment with a physical network. Option 5 is incorrect. AWS Global Accelerator is a service for improving network availability and performance by using the global AWS network, and does not increase the scalability of applications.

1. 48. Question

A company runs an e-commerce website on AWS. The website uses a public ALB and an EC2 instance in a private subnet. Static content is hosted on EC2 instances and dynamic content is pulled from RDS for Oracle. The company recently started selling to users in America and Europe. The application is running in Japan, but I want international users to be able to browse without delay. Which is the most cost effective solution?

* + Host your entire website on S3.
  + **Use CloudFront and S3 to host static content.**
  + Deploy your application in the Americas and Europe regions.
  + Increase the number of EC2 instances.

**Correct**

International users should be able to browse without delay. Therefore, it is important to choose a solution that can quickly display static content on your website to users visiting from overseas. Hosting static content using CloudFront and S3 is the most cost-effective and fastest way to access static content from around the world. So option 2 is the correct answer. Option 1 is incorrect. Not suitable as dynamic content cannot be hosted on S3. Option 3 is incorrect. Deploying applications in the US and European regions is not cost effective. Option 4 is incorrect. Increasing the number of EC2 instances is not cost effective.

1. 49. Question

A company is implementing a multi-region, disaster-recoverable relational database. Transactions to the database must ensure consistency and data integrity. In addition, the service level in the event of a database failure is defined as a recovery point objective (RPO) of 10 seconds and a recovery time objective (RTO) of 1 minute. Which AWS solution can fulfill this requirement?

* + DynamoDB global table
  + RDS for MySQL with Multi-AZ deployment enabled
  + RDS for MySQL with Cross-Region Snapshot Copy
  + **Aurora Global Database**

**Unattempted**

With Aurora Global Database, you can switch to the secondary region in less than a minute if the primary region fails. So option 4 is the correct answer. Option 1 is incorrect. In the case of the question, we are supposed to implement a relational database. This is incorrect because DynamoDB is not a relational database. Option 2 is incorrect. Multi-AZ deployments are meant to accommodate multiple AZs within the same region. It cannot handle region failures. Option 3 is incorrect. Cross-region snapshot copy of RDS can be used to restore databases across regions, but it cannot meet the RPO/RTO service level in the question.

1. 50. Question

A venture company runs a web application on AWS. A web application is running on multiple EC2 instances behind an ALB across multiple AZs in the us-east-1 region. The company is based I am planning to expand my points and would like to run my application in the new us-west-1 region. You need a solution with low latency and high availability as your base expands. what to do to answer this should I (Select one)

* + Run EC2 instance behind ALB in us-west-1 . Configure cross-zone load balancing in your ALB configuration.
  + Run an EC2 instance in us-west-1. Switch ALB to NLB to achieve cross-region load balancing.
  + **Run an EC2 instance behind an ALB in us-west-1. Configure Route 53 with a weighted routing policy. Create an alias record in Route 53 that points to your ALB.**
  + **Run an EC2 instance behind an ALB in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group containing load balancer endpoints in both regions.**

**Incorrect**

To run systems across multiple regions with low latency and high availability, creating accelerators with AWS Global Accelerator ensures that even as the number of EC2 instances running in us-west-1 scales, your environment Optimize your traffic on the backend without any changes and automatically reroute to available endpoints. Option 1 is incorrect. Cross-Zone Load Balancing is a service that evenly distributes load to EC2 instances registered across multiple AZs. Not for load balancing across regions. I don‘t. Option 2 is incorrect. Changing ALB to NLB. NLB is optimized to handle a large number of requests per second with low communication delays and to handle spike loads. solution. Not the best solution for load balancing across regions. Option 3 is incorrect. If the number of EC2 instances running in us-west-1 were to scale, the weighted routing policy would need to change, which would be costly to modify the network configuration.

1. 51. Question

You were tasked with building an EC2 instance capable of high-performance computing in order to create a physics computing system that analyzes natural phenomena. This instance requires low-latency, high-throughput networking and adequate storage capacity. Which EC2 instance launch option meets your requirements?

* + **Choose a cluster placement group when launching an EC2 instance.**
  + Choosing a partition placement group when launching an EC2 instance.
  + Choose a dedicated instance tenancy when launching an EC2 instance.
  + Select Dedicated Hosts when launching an EC2 instance.

**Unattempted**

Placement groups in EC2, described in options A and B, are options for grouping multiple EC2 instances together to improve network performance and mitigate hardware failures. A‘s cluster placement group can reduce network latency between instances in the same AZ and increase the maximum throughput. This makes it a great option for high-performance computing applications like your question. So option 1 is the correct answer. Option 2 is incorrect. By enabling partition placement groups, you distribute your instances across multiple logical partitions so that they do not share hardware with instances in other partitions. This is useful for large-scale distributed processing use cases like HDFS (Hadoop Distributed File System). Option 3 is incorrect. Dedicated instance tenancy, also known as Dedicated Instance, allows you to physically occupy one piece of hardware by selecting this option. This allows you to take advantage of applications that might otherwise be required by licensing or compliance standards to be physically installed on a single piece of hardware. Option 4 is incorrect. Dedicated host allows you to specify a host that is not possible with option 3. For example, you can specify the number of CPU cores, so use it when you want to start software with a core license agreement. Option 3 and Option 4 are both options that are independent of facility requirements.

1. 52. Question

After creating an AWS account, you started operating resources as a root user, but the security administrator pointed out a security risk. Which can eliminate the security risk? (Choose 2)

* + **Create an IAM user with permissions that match your purpose.**
  + Remove the root user and disable login functionality.
  + **Set up multi-factor authentication (MFA) for the root user.**
  + **Operate from the AWS CLI using the root user‘s access key and secret key.**
  + Operate from the management console using an EC2 key pair.

**Incorrect**

Best practice is to use IAM for normal operations after setting up multi-factor authentication (MFA) for the root user. After the initial setup of the AWS account, basically you will not be logged in as the root user. In addition, the MFA device and credentials set for the root user are strictly stored. So options 1 and 3 are correct. Option 2 is incorrect. The root user cannot be deleted. Option 4 is incorrect. Using the root user‘s access key and secret key is not recommended for security unless there is a specific reason to do so. Option 5 is incorrect. The EC2 key pair is used for login authentication when launching EC2. Resource operations cannot be performed with an EC2 key pair.

1. 53. Question

A company hosts its website on EC2 instances across multiple AZs. The company has an important press release scheduled for a specific date and time, and expects a spike in traffic at that time. It is necessary to change the settings so that the performance of the website does not deteriorate when the number of accesses suddenly increases. What suggestions does the solution architect have for meeting this requirement?

* + Use step scaling.
  + Use simple scaling.
  + **Use scheduled scaling.**
  + Use lifecycle hooks.

**Correct**

It‘s a matter of considering proper autoscaling settings. Scheduled scaling is used because of spikes in access and the time and date of the event that triggers the spike in access. So option 3 is the correct answer.

1. 54. Question

A company is migrating an Internet Information Services (IIS)-based web application running on multiple Windows servers to AWS. Currently, NAS (Network Attached Storage) is used so that the files used by this application can be accessed from multiple servers. Which AWS solution is the most durable for file sharing after migrating to AWS?

* + RDS
  + Storage Gateway
  + EFS
  + **Amazon FSx**

**Correct**

Amazon FSx is a managed storage service for EC2 on Windows. It can be mounted from multiple Windows servers and is used for file sharing. Choosing Multi-AZ when building Amazon FSx ensures fault tolerance. So option 4 is the correct answer. Option 1 is incorrect. RDS is a relational database solution. You can share data in RDS from multiple servers, but relational databases aren‘t great for sharing files. Option 2 is incorrect. Storage Gateway has a configuration in which the file system is on the on-premises side. It is not a service for sharing files on the AWS side server. Option 3 is incorrect. EFS is a file sharing service for Linux. Not supported on Windows instances.

1. 55. Question

You are designing a Lambda function that calls an API that retrieves a list of S3 buckets. What‘s the most secure way to give Lambda the permissions it needs?

* + Create an IAM user with the required permissions for Lambda. Create an IAM access key and secret key and store them in your Lambda function.
  + Create a Lambda function using an IAM user with permissions to list all S3 buckets.
  + Create an IAM user with the required permissions for Lambda. Create an IAM access key and secret key and store them in encrypted RDS. Get and use the IAM access key and secret key in RDS from the Lambda function.
  + **Create an IAM role with permissions to list all S3 buckets and attach it to your Lambda function.**

**Unattempted**

Use IAM Roles in AWS Identity and Access Management (IAM) to give your Lambda function access to AWS resources. Granular permissions for IAM roles can be achieved by attaching IAM policies that describe permission settings. So option 4 is the correct answer. Options 1 and 3 are incorrect. This is not recommended from a security point of view as it means keeping the IAM access key and secret key in the source code or database. Option 2 is incorrect. The permissions of the user who created the Lambda do not apply to the created Lambda.

1. 56. Question

A company has an e-commerce web application running on multiple EC2 instances. Recently, when a new product was launched, we had a problem with our web application‘s performance degrading due to a surge in traffic. The company plans to launch a new product next month. Management wants to scale the number of EC2 instances required for processing according to the traffic load from the product‘s launch. However, at that time, it is necessary to make settings so as not to set up useless EC2 instances as much as possible. What is the most efficient way to meet this requirement?

* + **Take advantage of Auto Scaling‘s gradual scaling policy.**
  + Take advantage of Auto Scaling scheduled scaling actions.
  + Add an EC2 Spot Instance.
  + **Increase the number of EC2 as Reserved Instances.**

**Incorrect**

The question is how to appropriately increase the number of EC2 instances according to the load. Auto Scaling‘s gradual scaling policy is suitable for determining the number of EC2 instances according to traffic load. In the gradual scaling policy, when the threshold is exceeded based on the value that can be obtained from CloudWatch metrics, add 1 unit if the usage rate of the obtained value is 60%, and add 2 units if the usage rate is 75%. You can specify the number of units to be scaled by the value, such as adding 4 units at 90%. Option 2 is incorrect. Like Option 1, we use Auto Scaling, but this option is not suitable for increasing or decreasing the number of instances depending on the load situation. Option 3 is incorrect. Spot Instances are cheaper than on-demand EC2 instances, so they are suitable for short-term temporary use, but EC2 instances may go down even during operation. Option 4 is incorrect. If you use Reserved Instances to lower the running cost of each EC2 instance, you can prepare a large number of instances at the same cost, but you can‘t flexibly increase or decrease depending on the load.

1. 57. Question

Your company is migrating applications and data from an on-premises environment to AWS. I need to move 300TB of application data to S3. Since we are a small company, our corporate network does not have a lot of bandwidth. Which solution would be the most cost-effective without impacting normal business operations?

* + Transfer data to S3 using the file gateway of Storage Gateway.
  + Put the data in the Snowmobile, transport it to AWS, and upload the data to S3.
  + **Put data in Snowball Edge, transport it to AWS, and upload data to S3.**
  + Use the Internet to transfer data to S3.

**Correct**

Snowball Edge is a service that allows you to transfer data to AWS using physical devices. AWS sends you a physical device that you can store your data in. You connect the device to your local network, fill it with data, and send it back to AWS. With this service, you can transfer data to AWS without straining your network bandwidth. The problem statement states that the network bandwidth is not high, so using Snowball Edge is a suitable solution to migrate data without affecting normal business operations. If you use Storage Gateway as in A, the normal network bandwidth will affect your business, so it will be necessary to increase the bandwidth. incur costs. So option 3 is the correct answer. Option 1 is incorrect. Storage Gateway uses a lot of network bandwidth because it has to use the internet to transfer files to S3. Option 2 is incorrect. Snowmobile is a service used when migrating exabyte-scale data to AWS, so it does not meet the requirements of the question. Option 4 is incorrect. Transfers over the Internet use a lot of network bandwidth.

1. 58. Question

A financial company manages transaction information in a database, and while transaction information is written frequently, reads must always return the latest state. The application occasionally generates reports on database data and joins across multiple tables. The database should automatically scale as the amount of data increases. Which AWS service meets your requirements?

* + **S3**
  + **Aurora**
  + DynamoDB
  + Redshift

**Incorrect**

Relational databases are a good choice to ensure data consistency for writes and reads. We also use Aurora due to our requirement to “scale automatically as the amount of data increases“. So option 2 is the correct answer. Option 1 is incorrect. S3 is suitable for storing large amounts of data at low cost, but for data processing, it must be combined with Athena or Lambda separately. Option 3 is incorrect. DynamoDB is a NoSQL service. By default, reading data immediately after writing is not guaranteed to return the latest state, and even if the strong consistency option is enabled, it may take some time to return the read result, so it does not meet the requirements. Option 4 is incorrect. Redshift is a data warehouse service, used for data analysis and visualization. Redshift does not have the ability to scale automatically.

1. 59. Question

You are a solution architect for a company. The system I‘m working on uses RDS (MySQL) and has a requirement to encrypt the data stored in RDS. Also, the encryption keys that encrypt your data must be rotated annually. Which solution meets these requirements?

* + **Enable RDS data encryption with AWS managed encryption keys. Encryption keys managed by AWS are automatically rotated.**
  + **Create a customer master key (CMK) in KMS for RDS data encryption and enable RDS data encryption on the CMK. Enable automatic CMK rotation.**
  + Create a customer master key (CMK) in KMS for RDS data encryption and enable RDS data encryption on the CMK. CMKs are rotated by default.
  + Enable RDS data encryption with AWS managed encryption keys. Enable AWS-managed encryption key rotation.

**Incorrect**

Both AWS managed encryption keys and KMS managed CMKs can implement encryption at rest. However, the rotation management of the RDS encryption key managed by AWS is not possible, so if you want to perform rotation management, you need to create a CMK for encryption in KMS and enable automatic rotation. So option 2 is the correct answer. Option 1 and option 4 are incorrect. Encryption keys managed by AWS cannot be rotated. Option 3 is incorrect. CMKs created in KMS are not rotated by default. To rotate, you must either do it manually or enable automatic rotation.

1. 60. Question

A solution architect is designing a mobile application to track expenses by capturing images of employee billing receipts. Two EC2 instances are installed as Web/AP servers on the front, and the load is distributed by CLB. EC2 instances are configured in an Auto Scaling group. I would like to store the receipt image data in S3 after authentication and virus check processing on EC2. Currently, uploading images via Web/AP servers generates a lot of traffic. What is the most efficient way to store receipt images from a mobile application in S3 while balancing the load?

* + Upload directly to S3 using a presigned URL.
  + Upload the image data to a second S3 bucket and have a Lambda event copy the image to the primary bucket.
  + **Increase the number of EC2 in the Web/AP server Auto Scaling group and write to S3 packets via the Web/AP server.**
  + Use Spot Instances to extend your Web/AP servers and provide resources for processing images.

**Correct**

This system authenticates the user on EC2, checks the images to be uploaded, and then stores the images in S3. In other words, it is necessary to perform processing on EC2 before uploading to S3. In cases like your question, Auto Scaling is used as a way to balance the EC2 load. The correct solution is to upload the images to EC2 load balanced by Auto Scaling, then process and store them in S3. Options 1 and 2 are incorrect. The receipt image data is directly uploaded to S3, but the problem statement states that authentication and virus check processing will be performed on EC2. Authentication with S3 or Lambda and virus check processing do not meet the requirements. Option 4 is incorrect. Spot Instances allow you to increase the lack of EC2 resources at a relatively low cost, but they are not suitable for your case as the EC2 instance may go down in the middle of processing.

1. 61. Question

Your department operates a website on-premises, but would like to analyze website user information on AWS. Analytics ingests your website‘s log files into AWS where your analytics team runs specific queries on a daily basis. The requirements for a new analytics solution to be built on AWS are to minimize data loss from on-premises data sources, to lighten the construction and operation load as much as possible, and to be able to execute data queries in near real time. Which combination of AWS services best meets these requirements?

* + **Build Kinesis Data Firehose to deliver streaming data from on-premises to S3. Query data stored in Redshift by loading data into a Redshift cluster.**
  + Build Kinesis Data Streams to deliver streaming data from on-premises to S3 Glacier. Query data using Kinesis Data Analytics.
  + Store data in S3 using Snowball. Query data using Athena.
  + **Modify the data source that stores the website log to be an EBS volume. Query data using Amazon Elasticsearch Service.**

**Incorrect**

Kinesis Data Firehose is a managed service that delivers streaming data to analytics tools and data stores. You can implement the process of importing log files like the question without building a complicated application. Also, Redshift is a data warehouse service provided by AWS that can accumulate large amounts of data and issue analytical queries. For Kinesis Data Firehose and Redshift integration, it is necessary to issue a COPY command from the S3 bucket to Redshift in order to load the log data into the Redshift cluster. So Option 1, which combines these, is the correct answer. Option 2 is incorrect. Kinesis Data Streams can perform millisecond-level real-time processing, so it is a suitable service for requirements that require more real-time performance, but it is necessary to implement the processing for ingesting data. Therefore, Kinesis Data Firehose is relatively suitable in light of the question‘s requirements of reducing the construction and operation load and near real time. In addition, S3 Glacier is used as the storage destination for log data, which is a service used for low-cost, long-term storage. It is not suitable as a storage destination for logs that are frequently analyzed, as it takes time and money to retrieve the data. Option 3 is incorrect. Snowball is a service that migrates large amounts of data exceeding terabytes to AWS using physical devices. The question does not require the web service itself to be migrated to AWS, and there is no need to migrate the user data to be analyzed. Option 4 is incorrect. You cannot use EBS mounted on your on-premises website server.

1. 62. Question

Your company has decided to give everyone in your IT department access to your AWS account. The internal system uses an on-premises LDAP (Lightweight Directory Access Protocol) directory service for authentication. We would like to be able to use the same authentication as our internal system for single sign-on to the AWS Management Console. How can I do that? (Choose 2)

* + **Use IAM roles to set permissions for users federated from your identity provider (IdP).**
  + **Enable single sign-on with identity federation using SAML 2.0.**
  + Start EC2 for authentication information federation and set it to work with on-premises LDAP and credentials.
  + In your organization‘s IdP, map your organization‘s users or groups to IAM users.
  + **Integrate Cognito with an on-premises LDAP directory service.**

**Incorrect**

AWS supports identity federation using SAML 2.0. You can use this feature to achieve single sign-on (SSO) to the AWS Management Console. With SSO, you don‘t need to create individual IAM users for everyone in your organization to log in to the AWS Management Console and perform various operations. To achieve SSO to the AWS Management Console using your on-premises credentials, use your on-premises Identity Provider (IdP) and AWS‘s SSO endpoint. When a user accesses the portal, the IdP authenticates the user and returns a SAML assertion, which is a metadata document describing the user‘s credentials, attributes, etc. When a client, such as a browser, POSTs a SAML assertion to an AWS SSO endpoint, the SSO endpoint obtains temporary credentials from the STS. The SSO endpoint generates a redirect URL to return the AWS Management Console URL to the client. Clients can use this URL to access the AWS Management Console. Permissions on the AWS Management Console are determined by IAM roles that are pre-associated with SAML assertion attributes. So option 1 and option 2 are correct.

1. 63. Question

A company operates a mobile chat application. We use DynamoDB for our application database. We are currently considering additional development of the application and would like to load messages faster than ever before. In addition, it is necessary to keep application changes to a minimum for additional development. Which is the best way to meet these requirements?

* + Add DynamoDB read replicas to handle the increased read load. Update your application to point to the read replica‘s read endpoint.
  + **Configure DynamoDB Accelerator (DAX) for your new message table and update your application to use the DAX endpoint.**
  + **Add ElastiCache for Redis to your application stack. Update your application to point to your Redis cache endpoint.**
  + Double your DynamoDB read capacity units. Continue to use your existing DynamoDB endpoints.

**Incorrect**

This question asks you to improve DynamoDB read speeds with minimal changes to your application. By using DynamoDB Accelerator (DAX), the messages required for reading can be cached within DynamoDB, improving read speed. DAX is also compatible with DynamoDB, so you can minimize application changes. So option 2 is the correct answer. Option 1 is incorrect. RDS can use read replicas, but DynamoDB cannot. Option 3 is incorrect. Introducing a caching mechanism using ElastiCache for Redis improves read performance, but requires significant changes compared to Option 2. Option 4 is incorrect. Increasing the read capacity unit increases read throughput, but does not increase read speed.

1. 64. Question

Your company uses ECS to operate an image processing application. The images are stored in an S3 bucket. The ECS that reads the images is in two private subnets and accesses S3 over the Internet via a NAT instance on each private subnet. A recent cost study points to the rising cost of network communication over the Internet. Change to cost-optimal architecture Which solution is right for you?

* + **Change the access route from the private subnet to S3 via a gateway type VPC endpoint.**
  + Place ECS in a public subnet.
  + Change a NAT instance to a NAT gateway.
  + Change ECS to EC2.

**Correct**

When accessing S3, which is a global service, from EC2 or ECS placed within a VPC, it is usually necessary to access via the Internet. However, if you use a gateway-type VPC endpoint, you will be able to access S3 directly from the private network within the VPC via the network within AWS, without going through the Internet. In this case, you can save the cost of outbound communication to the Internet, NAT gateway, NAT instance, etc.

1. 65. Question

A company runs multiple websites for different business lines. Users accessing these websites are routed to the appropriate backend EC2 instance based on the subdomain they access. Websites run server-side scripts such as static web pages, images, PHP, and JavaScript. Some websites experience peak traffic within two hours of opening, with constant traffic for the rest of the day. You need to design a solution that automatically adjusts capacity to these traffic patterns while keeping costs low. Which AWS services or features together meet these requirements? (Choose 2)

* + **AWS Batch**
  + NLBMore
  + **ALB**
  + **EC2 Auto Scaling**
  + **S3 static website hosting**

**Incorrect**

This question has two points. One is the ability to perform appropriate routing based on the subdomain being accessed, and the other is the ability to automatically adjust capacity to match traffic patterns. ALB is best for routing per subdomain you visit. Also, use EC2 Auto Scaling to automatically adjust the number of servers dynamically according to the load. So options 3 and 4 are correct. Option 1 is incorrect. AWS Batch is a service used for batch processing. It does not increase EC2 according to the load of the web system. Option 2 is incorrect. NLB does not allow per-domain routing. Option 5 is incorrect. Dynamic resources cannot be placed on S3.