

Practice Test #2 - AWS Certified Solutions Architect Associate

Pregunta 1:

You have a team of developers in your company, and you would like to ensure they can quickly experiment with AWS Managed Policies by attaching them to their accounts, but you would like to prevent them from doing an escalation of privileges, by granting themselves the `AdministratorAccess` managed policy. How should you proceed?

- Put the developers into an IAM group, and then define an IAM permission boundary on the group that will restrict the managed policies they can attach to themselves
- Attach an IAM policy to your developers, that prevents them from attaching the `AdministratorAccess` policy
- Create a Service Control Policy (SCP) on your AWS account that restricts developers from attaching themselves the `AdministratorAccess` policy
- For each developer, define an IAM permission boundary that will restrict the managed policies they can attach to themselves

Pregunta 2:

A developer needs to implement a Lambda function in AWS account A that accesses an Amazon S3 bucket in AWS account B.

As a Solutions Architect, which of the following will you recommend to meet this requirement?

- **The S3 bucket owner should make the bucket public so that it can be accessed by the Lambda function in the other AWS account**
- **Create an IAM role for the Lambda function that grants access to the S3 bucket. Set the IAM role as the Lambda function's execution role and that would give the Lambda function cross-account access to the S3 bucket**
- **Create an IAM role for the Lambda function that grants access to the S3 bucket. Set the IAM role as the Lambda function's execution role. Make sure that the bucket policy also grants access to the Lambda function's execution role**
- **AWS Lambda cannot access resources across AWS accounts. Use Identity federation to work around this limitation of Lambda**

Pregunta 3:

A systems administrator has created a private hosted zone and associated it with a Virtual Private Cloud (VPC). However, the DNS queries for the private hosted zone remain unresolved.

As a Solutions Architect, can you identify the Amazon VPC options to be configured in order to get the private hosted zone to work?

- **Fix conflicts between your private hosted zone and any Resolver rule that routes traffic to your network for the same domain name, as it results in ambiguity over the route to be taken**
- **Fix the Name server (NS) record and Start Of Authority (SOA) records that may have been created with wrong configurations**
- **Remove any overlapping namespaces for the private and public hosted zones**
- **Enable DNS hostnames and DNS resolution for private hosted zones**

Pregunta 4:

Upon a security review of your AWS account, an AWS consultant has found that a few RDS databases are un-encrypted. As a Solutions Architect, what steps must be taken to encrypt the RDS databases?

- **Enable Multi-AZ for the database, and make sure the standby instance is encrypted. Stop the main database to that the standby database kicks in, then disable Multi-AZ**
- **Enable encryption on the RDS database using the AWS Console**
- **Create a Read Replica of the database, and encrypt the read replica. Promote the read replica as a standalone database, and terminate the previous database**
- **Take a snapshot of the database, copy it as an encrypted snapshot, and restore a database from the encrypted snapshot. Terminate the previous database**

Pregunta 5:

A cybersecurity company uses a fleet of EC2 instances to run a proprietary application. The infrastructure maintenance group at the company wants to be notified via an email whenever the CPU utilization for any of the EC2 instances breaches a certain threshold.

Which of the following services would you use for building a solution with the LEAST amount of development effort? (Select two)

- **AWS Lambda**
- **Amazon SQS**
- **Amazon CloudWatch**
- **Amazon SNS**
- **AWS Step Functions**

Pregunta 6:

An analytics company wants to improve the performance of its big data processing workflows running on Amazon EFS. Which of the following performance modes should be used for EFS to address this requirement?

- **General Purpose**
- **Max I/O**
- **Provisioned Throughput**
- **Bursting Throughput**

Pregunta 7:

An IT company is working on client engagement to build a real-time data analytics tool for the Internet of Things (IoT) data. The IoT data is funneled into Kinesis Data Streams which further acts as the source of a delivery stream for Kinesis Firehose. The engineering team has now configured a Kinesis Agent to send IoT data from another set of devices to the same Firehose delivery stream. They noticed that data is not reaching Firehose as expected.

As a solutions architect, which of the following options would you attribute as the MOST plausible root cause behind this issue?

- **The data sent by Kinesis Agent is lost because of a configuration error**
- **Kinesis Agent cannot write to a Kinesis Firehose for which the delivery stream source is already set as Kinesis Data Streams**
- **Kinesis Agent can only write to Kinesis Data Streams, not to Kinesis Firehose**
- **Kinesis Firehose delivery stream has reached its limit and needs to be scaled manually**

Pregunta 8:

A company is looking at storing their less frequently accessed files on AWS that can be concurrently accessed by hundreds of EC2 instances. The company needs the most cost-effective file storage service that provides immediate access to data whenever needed.

Which of the following options represents the best solution for the given requirements?

- **Amazon Elastic File System (EFS) Standard storage class**
- **Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class**
- **Amazon Elastic Block Store (EBS)**
- **Amazon Elastic File System (EFS) Standard-IA storage class**

Pregunta 9

Which of the following IAM policies provides read-only access to the S3 bucket `mybucket` and its content?

1.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::mybucket"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::mybucket/*"
    }
  ]
}
```

2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::mybucket"
    }
  ]
}
```

3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::mybucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
    "s3:GetObject"
  ],
  "Resource": "arn:aws:s3:::mybucket"
}
]
```

4.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::mybucket/*"
    }
  ]
}
```

Pregunta 10:

Your company has an on-premises Distributed File System Replication (DFSR) service to keep files synchronized on multiple Windows servers, and would like to migrate to AWS cloud.

What do you recommend as a replacement for the DFSR?

- **Amazon S3**
- **FSx for Lustre**
- **EFS**
- **FSx for Windows**

Pregunta 11:

A Machine Learning research group uses a proprietary computer vision application hosted on an EC2 instance. Every time the instance needs to be stopped and started again, the application takes about 3 minutes to start as some auxiliary software programs need to be executed so that the application can function. The research group would like to minimize the application bootstrap time whenever the system needs to be stopped and then started at a later point in time.

As a solutions architect, which of the following solutions would you recommend for this use-case?

- **Use EC2 Instance Hibernate**
- **Create an AMI and launch your EC2 instances from that**
- **Use EC2 Meta-Data**
- **Use EC2 User-Data**

Pregunta 12:

Amazon EC2 Auto Scaling needs to terminate an instance from Availability Zone (AZ) `us-east-1a` as it has the most number of instances amongst the AZs being used currently. There are 4 instances in the AZ `us-east-1a` like so: Instance A has the oldest launch template, Instance B has the oldest launch configuration, Instance C has the newest launch configuration and Instance D is closest to the next billing hour.

Which of the following instances would be terminated per the default termination policy?

- **Instance B**
- **Instance C**
- **Instance D**
- **Instance A**

Pregunta 13:

You have multiple AWS accounts within a single AWS Region managed by AWS Organizations and you would like to ensure all EC2 instances in all these accounts can communicate privately. Which of the following solutions provides the capability at the CHEAPEST cost?

- **Create a VPC in an account and share one or more of its subnets with the other accounts using Resource Access Manager**
- **Create a Private Link between all the EC2 instances**
- **Create a Transit Gateway and link all the VPC in all the accounts together**
- **Create a VPC peering connection between all VPCs**

Pregunta 14:

What does this IAM policy do?

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "34.50.31.0/24"
        }
      }
    }
  ]
}
```

- It allows starting EC2 instances only when they have a Public IP within the 34.50.31.0/24 CIDR block
- It allows starting EC2 instances only when they have an Elastic IP within the 34.50.31.0/24 CIDR block
- It allows starting EC2 instances only when the IP where the call originates is within the 34.50.31.0/24 CIDR block
- It allows starting EC2 instances only when they have a Private IP within the 34.50.31.0/24 CIDR block

Pregunta 15:

You would like to use Snowball to move on-premises backups into a long term archival tier on AWS. Which solution provides the MOST cost savings?

- **Create a Snowball job and target an S3 bucket. Create a lifecycle policy to transition this data to Glacier Deep Archive on the same day**
- **Create a Snowball job and target a Glacier Deep Archive Vault**
- **Create a Snowball job and target an S3 bucket. Create a lifecycle policy to transition this data to Glacier on the same day**
- **Create a Snowball job and target a Glacier Vault**

Pregunta 16

A big data consulting firm needs to set up a data lake on Amazon S3 for a Health-Care client. The data lake is split in raw and refined zones. For compliance reasons, the source data needs to be kept for a minimum of 5 years. The source data arrives in the raw zone and is then processed via an AWS Glue based ETL job into the refined zone. The business analysts run ad-hoc queries only on the data in the refined zone using AWS Athena. The team is concerned about the cost of data storage in both the raw and refined zones as the data is increasing at a rate of 1TB daily in each zone.

As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution? (Select two)

- **Setup a lifecycle policy to transition the raw zone data into Glacier Deep Archive after 1 day of object creation**
- **Setup a lifecycle policy to transition the refined zone data into Glacier Deep Archive after 1 day of object creation**
- **Create a Lambda function based job to delete the raw zone data after 1 day**
- **Use Glue ETL job to write the transformed data in the refined zone using CSV format**
- **Use Glue ETL job to write the transformed data in the refined zone using a compressed file format(Correcto)**

Pregunta 17:

A media company has created an AWS Direct Connect connection for migrating its flagship application to the AWS Cloud. The on-premises application writes hundreds of video files into a mounted NFS file system daily. Post-migration, the company will host the application on an Amazon EC2 instance with a mounted EFS file system. Before the migration cutover, the company must build a process that will replicate the newly created on-premises video files to the EFS file system.

Which of the following represents the MOST operationally efficient way to meet this requirement?

- **Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the Direct Connect connection to an S3 bucket by using public VIF. Set up an AWS Lambda function to process event notifications from Amazon S3 and copy the video files from Amazon S3 to the EFS file system**
- **Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the Direct Connect connection to an S3 bucket by using an S3 VPC endpoint. Set up an AWS Lambda function to process event notifications from Amazon S3 and copy the video files from Amazon S3 to the EFS file system**
- **Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Set up a DataSync scheduled task to send the video files to the EFS file system every 24 hours**

- **Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the Direct Connect connection to an AWS VPC peering endpoint for Amazon EFS by using a private VIF. Set up a DataSync scheduled task to send the video files to the EFS file system every 24 hours**

Pregunta 18:

You would like to store a database password in a secure place, and enable automatic rotation of that password every 90 days. What do you recommend?

- **Key Management Service (KMS)**
- **SSM Parameter Store**
- **Secrets Manager**
- **CloudHSM**

Pregunta 19:

To improve the performance and security of the application, the engineering team at a company has created a CloudFront distribution with an Application Load Balancer as the custom origin. The team has also set up a Web Application Firewall (WAF) with CloudFront distribution. The security team at the company has noticed a surge in malicious attacks from a specific IP address to steal sensitive data stored on the EC2 instances.

As a solutions architect, which of the following actions would you recommend to stop the attacks?

- **Create an IP match condition in the WAF to block the malicious IP address**
- **Create a ticket with AWS support to take action against the malicious IP**
- **Create a deny rule for the malicious IP in the Security Groups associated with each of the instances**
- **Create a deny rule for the malicious IP in the NACL associated with each of the instances**

Pregunta 20:

You would like to migrate an AWS account from an AWS Organization A to an AWS Organization B. What are the steps do to it?

- **Send an invite to the new organization. Accept the invite to the new organization from the member account. Remove the member account from the old organization**
- **Open an AWS Support ticket to ask them to migrate the account**
- **Send an invite to the new organization. Remove the member account from the old organization. Accept the invite to the new organization from the member account**
- **Remove the member account from the old organization. Send an invite to the member account from the new Organization. Accept the invite to the new organization from the member account**

Pregunta 21:

A financial services company wants a single log processing model for all the log files (consisting of system logs, application logs, database logs, etc) that can be processed in a serverless fashion and then durably stored for downstream analytics. The company wants to use an AWS managed service that automatically scales to match the throughput of the log data and requires no ongoing administration.

As a solutions architect, which of the following AWS services would you recommend solving this problem?

- **Kinesis Data Streams**
- **AWS Lambda**
- **Kinesis Data Firehose**
- **Amazon EMR**

Pregunta 22:

A silicon valley based startup has a content management application with the web-tier running on EC2 instances and the database tier running on Amazon Aurora. Currently, the entire infrastructure is located in us-east-1 region. The startup has 90% of its customers in the US and Europe. The engineering team is getting reports of deteriorated application performance from customers in Europe with high application load time.

As a solutions architect, which of the following would you recommend addressing these performance issues? (Select two)

- **Create Amazon Aurora read replicas in the eu-west-1 region**
- **Create Amazon Aurora Multi-AZ standby instance in the eu-west-1 region**
- **Setup another fleet of EC2 instances for the web tier in the eu-west-1 region. Enable failover routing policy in Route 53**
- **Setup another fleet of EC2 instances for the web tier in the eu-west-1 region. Enable latency routing policy in Route 53**
- **Setup another fleet of EC2 instances for the web tier in the eu-west-1 region. Enable geolocation routing policy in Route 53**

Pregunta 23:

A company has recently launched a new mobile gaming application that the users are adopting rapidly. The company uses RDS MySQL as the database. The engineering team wants an urgent solution to this issue where the rapidly increasing workload might exceed the available database storage.

As a solutions architect, which of the following solutions would you recommend so that it requires minimum development and systems administration effort to address this requirement?

- **Enable storage auto-scaling for RDS MySQL**
- **Create read replica for RDS MySQL**
- **Migrate RDS MySQL database to Aurora which offers storage auto-scaling**
- **Migrate RDS MySQL database to DynamoDB which automatically allocates storage space when required**

Pregunta 24:

An e-commerce application uses an Amazon Aurora Multi-AZ deployment for its database. While analyzing the performance metrics, the engineering team has found that the database reads are causing high I/O and adding latency to the write requests against the database.

As an AWS Certified Solutions Architect Associate, what would you recommend to separate the read requests from the write requests?

- **Provision another Amazon Aurora database and link it to the primary database as a read replica**
- **Activate read-through caching on the Amazon Aurora database**
- **Set up a read replica and modify the application to use the appropriate endpoint**
- **Configure the application to read from the Multi-AZ standby instance**

Pregunta 25:

An IT company has built a solution wherein a Redshift cluster writes data to an Amazon S3 bucket belonging to a different AWS account. However, it is found that the files created in the S3 bucket using the UNLOAD command from the Redshift cluster are not even accessible to the S3 bucket owner.

What could be the reason for this denial of permission for the bucket owner?

- **When two different AWS accounts are accessing an S3 bucket, both the accounts must share the bucket policies. An erroneous policy can lead to such permission failures**
- **When objects are uploaded to S3 bucket from a different AWS account, the S3 bucket owner will get implicit permissions to access these objects. This issue seems to be due to an upload error that can be fixed by providing manual access from AWS console**
- **By default, an S3 object is owned by the AWS account that uploaded it. So the S3 bucket owner will not implicitly have access to the objects written by the Redshift cluster**
- **The owner of an S3 bucket has implicit access to all objects in his bucket. Permissions are set on objects after they are completely copied to the target location. Since the owner is unable to access the uploaded files, the write operation may be still in progress**

Pregunta 26:

You are establishing a monitoring solution for desktop systems, that will be sending telemetry data into AWS every 1 minute. Data for each system must be processed in order, independently, and you would like to scale the number of consumers to be possibly equal to the number of desktop systems that are being monitored.

What do you recommend?

- **Use an SQS standard queue, and send the telemetry data as is**
- **Use an SQS FIFO queue, and send the telemetry data as is**
- **Use a Kinesis Data Stream, and send the telemetry data with a Partition ID that uses the value of the Desktop ID**
- **Use an SQS FIFO queue, and make sure the telemetry data is sent with a Group ID attribute representing the value of the Desktop ID**

Pregunta 27:

A junior DevOps engineer wants to change the default configuration for EBS volume termination. By default, the root volume of an EC2 instance for an EBS-backed AMI is deleted when the instance terminates.

Which option below helps change this default behavior to ensure that the volume persists even after the instance terminates?

- **Set the DeleteOnTermination attribute to true**
- **Set the DeleteOnTermination attribute to false**
- **Set the TerminateOnDelete attribute to true**
- **Set the TerminateOnDelete attribute to false**

Pregunta 28:

A financial services company has developed its flagship application on AWS Cloud with data security requirements such that the encryption key must be stored in a custom application running on-premises. The company wants to offload the data storage as well as the encryption process to Amazon S3 but continue to use the existing encryption key.

Which of the following S3 encryption options allows the company to leverage Amazon S3 for storing data with given constraints?

- **Client-Side Encryption with data encryption is done on the client-side before sending it to Amazon S3**
- **Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)**
- **Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)**
- **Server-Side Encryption with Customer-Provided Keys (SSE-C)**

Pregunta 29:

An application runs big data workloads on EC2 instances. The application runs 24x7 all round the year and needs at least 20 instances to maintain a minimum acceptable performance threshold and the application needs 300 instances to handle spikes in the workload. Based on historical workloads processed by the application, it needs 80 instances 80% of the time.

As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution so that it can meet the workload demand in a steady state?

- **Purchase 80 spot instances. Use Auto Scaling Group to provision the remaining instances as on-demand instances per the workload demand**
- **Purchase 80 on-demand instances. Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with launch template to provision the mix of on-demand and spot instances)**
- **Purchase 80 reserved instances. Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with launch template to provision the mix of on-demand and spot instances)**
- **Purchase 20 on-demand instances. Use Auto Scaling Group to provision the remaining instances as spot instances per the workload demand**

Pregunta 30:

Your company has a monthly big data workload, running for about 2 hours, which can be efficiently distributed across multiple servers of various sizes, with a variable number of CPUs. The solution for the workload should be able to withstand server failures.

Which is the MOST cost-optimal solution for this workload?

- **Run the workload on a Spot Fleet**
- **Run the workload on Reserved Instances**
- **Run the workload on Dedicated Hosts**
- **Run the workload on Spot Instances**

Pregunta 31:

A Hollywood studio is planning a series of promotional events leading up to the launch of the trailer of its next sci-fi thriller. The executives at the studio want to create a static website with lots of animations in line with the theme of the movie. The studio has hired you as a solutions architect to build a scalable serverless solution.

Which of the following represents the MOST cost-optimal and high-performance solution?

- **Build the website as a static website hosted on Amazon S3. Create a CloudFront distribution with Amazon S3 as the origin. Use Amazon Route 53 to create an alias record that points to your CloudFront distribution**
- **Host the website on AWS Lambda. Create a CloudFront distribution with Lambda as the origin**
- **Host the website on an EC2 instance. Create a CloudFront distribution with the EC2 instance as the custom origin**
- **Host the website on an instance in the studio's on-premises data center. Create a CloudFront distribution with this instance as the custom origin**

Pregunta 32:

A financial services company has deployed its flagship application on EC2 instances. Since the application handles sensitive customer data, the security team at the company wants to ensure that any third-party SSL/TLS certificates configured on EC2 instances via the AWS Certificate Manager (ACM) are renewed before their expiry date. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution that notifies the security team 30 days before the certificate expiration. The solution should require the least amount of scripting and maintenance effort.

What will you recommend?

- **Leverage AWS Config managed rule to check if any SSL/TLS certificates created via ACM are marked for expiration within 30 days. Configure the rule to trigger an SNS notification to the security team if any certificate expires within 30 days**
- **Leverage AWS Config managed rule to check if any third-party SSL/TLS certificates imported into ACM are marked for expiration within 30 days. Configure the rule to trigger an SNS notification to the security team if any certificate expires within 30 days**
- **Monitor the `days to expiry` CloudWatch metric for certificates created via ACM. Create a CloudWatch alarm to monitor such certificates based on the `days to expiry` metric and then trigger a custom action of notifying the security team**
- **Monitor the `days to expiry` CloudWatch metric for certificates imported into ACM. Create a CloudWatch alarm to monitor such certificates based on the `days to expiry` metric and then trigger a custom action of notifying the security team**

Pregunta 33:

A silicon valley based startup has a two-tier architecture using EC2 instances for its flagship application. The web servers (listening on port 443), which have been assigned security group A, are in public subnets across two Availability Zones and the MSSQL based database instances (listening on port 1433), which have been assigned security group B, are in two private subnets across two Availability Zones. The DevOps team wants to review the security configurations of the application architecture.

As a solutions architect, which of the following options would you select as the MOST secure configuration? (Select two)

- **For security group A: Add an inbound rule that allows traffic from all sources on port 443. Add an outbound rule with the destination as security group B on port 443**
- **For security group B: Add an inbound rule that allows traffic only from security group A on port 1433**
- **For security group A: Add an inbound rule that allows traffic from all sources on port 443. Add an outbound rule with the destination as security group B on port 1433**
- **For security group B: Add an inbound rule that allows traffic only from all sources on port 1433**
- **For security group B: Add an inbound rule that allows traffic only from security group A on port 443**

Pregunta 34:

An IT company wants to optimize the costs incurred on its fleet of 100 EC2 instances for the next year. Based on historical analyses, the engineering team observed that 70 of these instances handle the compute services of its flagship application and need to be always available. The other 30 instances are used to handle batch jobs that can afford a delay in processing.

As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution?

- **Purchase 70 reserved instances and 30 on-demand instances**
- **Purchase 70 reserved instances and 30 spot instances**
- **Purchase 70 on-demand instances and 30 spot instances**
- **Purchase 70 on-demand instances and 30 reserved instances**

Pregunta 35:

A big-data consulting firm is working on a client engagement where the ETL workloads are currently handled via a Hadoop cluster deployed in the on-premises data center. The client wants to migrate their ETL workloads to AWS Cloud. The AWS Cloud solution needs to be highly available with about 50 EC2 instances per Availability Zone.

As a solutions architect, which of the following EC2 placement groups would you recommend handling the distributed ETL workload?

- **Partition placement group**
- **Cluster placement group**
- **Both Spread placement group and Partition placement group**
- **Spread placement group**

Pregunta 36:

Your company has deployed an application that will perform a lot of overwrites and deletes on data and require the latest information to be available anytime data is read via queries on database tables.

As a Solutions Architect, which database technology will you recommend?

- **Amazon Relational Database Service (Amazon RDS)**
- **Amazon Simple Storage Service (Amazon S3)**
- **Amazon Neptune**
- **Amazon ElastiCache**

Pregunta 37:

A retail company wants to rollout and test a blue-green deployment for its global application in the next 48 hours. Most of the customers use mobile phones which are prone to DNS caching. The company has only two days left for the annual Thanksgiving sale to commence.

As a Solutions Architect, which of the following options would you recommend to test the deployment on as many users as possible in the given time frame?

- **Use Elastic Load Balancer to distribute traffic across deployments**
- **Use Route 53 weighted routing to spread traffic across different deployments**
- **Use AWS Global Accelerator to distribute a portion of traffic to a particular deployment**
- **Use AWS CodeDeploy deployment options to choose the right deployment**

Pregunta 38:

A manufacturing company receives unreliable service from its data center provider because the company is located in an area prone to natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failover environment on AWS in case the on-premises data center fails. The company runs web servers that connect to external vendors. The data available on AWS and on-premises must be uniform.

Which of the following solutions would have the LEAST amount of downtime?

- **Set up a Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer**
- **Set up a Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to S3. Set up an AWS Direct Connect connection between a VPC and the data center**
- **Set up a Route 53 failover record. Execute an AWS CloudFormation template from a script to provision EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to S3**
- **Set up a Route 53 failover record. Run application servers on EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to S3**

Pregunta 39:

The engineering manager for a content management application wants to set up RDS read replicas to provide enhanced performance and read scalability. The manager wants to understand the data transfer charges while setting up RDS read replicas.

Which of the following would you identify as correct regarding the data transfer charges for RDS read replicas?

- **There are data transfer charges for replicating data across AWS Regions**
- **There are no data transfer charges for replicating data across AWS Regions**
- **There are data transfer charges for replicating data within the same Availability Zone**
- **There are data transfer charges for replicating data within the same AWS Region**

Pregunta 40:

An engineering team wants to examine the feasibility of the `user data` feature of Amazon EC2 for an upcoming project.

Which of the following are true about the EC2 user data configuration? (Select two)

- **When an instance is running, you can update user data by using root user credentials**
- **By default, scripts entered as user data are executed with root user privileges**
- **By default, scripts entered as user data do not have root user privileges for executing**
- **By default, user data runs only during the boot cycle when you first launch an instance**
- **By default, user data is executed every time an EC2 instance is re-started**

Pregunta 41:

An IT company provides S3 bucket access to specific users within the same account for completing project specific work. With changing business requirements, cross-account S3 access requests are also growing every month. The company is looking for a solution that can offer user level as well as account-level access permissions for the data stored in S3 buckets.

As a Solutions Architect, which of the following would you suggest as the MOST optimized way of controlling access for this use-case?

- **Use Amazon S3 Bucket Policies**
- **Use Access Control Lists (ACLs)**
- **Use Security Groups**
- **Use Identity and Access Management (IAM) policies**

Pregunta 42:

You have been hired as a Solutions Architect to advise a company on the various authentication/authorization mechanisms that AWS offers to authorize an API call within the API Gateway. The company would prefer a solution that offers built-in user management.

Which of the following solutions would you suggest as the best fit for the given use-case?

- **Use API Gateway Lambda authorizer**
- **Use AWS_IAM authorization**
- **Use Amazon Cognito Identity Pools**
- **Use Amazon Cognito User Pools**

Pregunta 43:

A financial services company wants to store confidential data in Amazon S3 and it needs to meet the following data security and compliance norms:

1. Encryption key usage must be logged for auditing purposes
2. Encryption Keys must be rotated every year
3. The data must be encrypted at rest

Which is the MOST operationally efficient solution?

- **Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual key rotation**
- **Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic key rotation**
- **Server-side encryption (SSE-S3) with automatic key rotation**
- **Server-side encryption with customer-provided keys (SSE-C) with automatic key rotation**

Pregunta 44:

What does this IAM policy do?

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "eu-west-1"
        }
      }
    }
  ]
}
```

- It allows running EC2 instances in any region when the API call is originating from the eu-west-1 region
- It allows to run EC2 instances in the eu-west-1 region, when the API call is made from the eu-west-1 region
- It allows running EC2 instances anywhere but in the eu-west-1 region

- **It allows running EC2 instances only in the eu-west-1 region, and the API call can be made from anywhere in the world**

Pregunta 45:

An IT company has an Access Control Management (ACM) application that uses Amazon RDS for MySQL but is running into performance issues despite using Read Replicas. The company has hired you as a solutions architect to address these performance-related challenges without moving away from the underlying relational database schema. The company has branch offices across the world, and it needs the solution to work on a global scale.

Which of the following will you recommend as the MOST cost-effective and high-performance solution?

- **Use Amazon Aurora Global Database to enable fast local reads with low latency in each region**
- **Spin up a Redshift cluster in each AWS region. Migrate the existing data into Redshift clusters**
- **Use Amazon DynamoDB Global Tables to provide fast, local, read and write performance in each region**
- **Spin up EC2 instances in each AWS region, install MySQL databases and migrate the existing data into these new databases**

Pregunta 46:

A social photo-sharing web application is hosted on EC2 instances behind an Elastic Load Balancer. The app gives the users the ability to upload their photos and also shows a leaderboard on the homepage of the app. The uploaded photos are stored in S3 and the leaderboard data is maintained in DynamoDB. The EC2 instances need to access both S3 and DynamoDB for these features.

As a solutions architect, which of the following solutions would you recommend as the MOST secure option?

- **Configure AWS CLI on the EC2 instances using a valid IAM user's credentials. The application code can then invoke shell scripts to access S3 and DynamoDB via AWS CLI**
- **Attach the appropriate IAM role to the EC2 instance profile so that the instance can access S3 and DynamoDB**
- **Save the AWS credentials (access key Id and secret access token) in a configuration file within the application code on the EC2 instances. EC2 instances can use these credentials to access S3 and DynamoDB**
- **Encrypt the AWS credentials via a custom encryption library and save it in a secret directory on the EC2 instances. The application code can then safely decrypt the AWS credentials to make the API calls to S3 and DynamoDB**

Pregunta 47:

A company has many VPC in various accounts, that need to be connected in a star network with one another and connected with on-premises networks through Direct Connect.

What do you recommend?

- **Transit Gateway**
- **VPC Peering**
- **Private Link**
- **VPN Gateway**

Pregunta 48:

An application is currently hosted on four EC2 instances (behind Application Load Balancer) deployed in a single Availability Zone (AZ). To maintain an acceptable level of end-user experience, the application needs at least 4 instances to be always available.

As a solutions architect, which of the following would you recommend so that the application achieves high availability with MINIMUM cost?

- **Deploy the instances in one Availability Zones. Launch two instances in the Availability Zone**
- **Deploy the instances in two Availability Zones. Launch four instances in each Availability Zone**
- **Deploy the instances in two Availability Zones. Launch two instances in each Availability Zone**
- **Deploy the instances in three Availability Zones. Launch two instances in each Availability Zone**

Pregunta 49:

A weather forecast agency collects key weather metrics across multiple cities in the US and sends this data in the form of key-value pairs to AWS Cloud at a one-minute frequency.

As a solutions architect, which of the following AWS services would you use to build a solution for processing and then reliably storing this data with high availability? (Select two)

- **Redshift**
- **DynamoDB**
- **Lambda**
- **RDS**
- **ElastiCache**

Pregunta 50:

A developer has configured inbound traffic for the relevant ports in both the Security Group of the EC2 instance as well as the Network Access Control List (NACL) of the subnet for the EC2 instance. The developer is, however, unable to connect to the service running on the Amazon EC2 instance.

As a solutions architect, how will you fix this issue?

- **Rules associated with Network ACLs should never be modified from command line. An attempt to modify rules from command line blocks the rule and results in an erratic behavior**
- **Network ACLs are stateful, so allowing inbound traffic to the necessary ports enables the connection. Security Groups are stateless, so you must allow both inbound and outbound traffic**
- **Security Groups are stateful, so allowing inbound traffic to the necessary ports enables the connection. Network ACLs are stateless, so you must allow both inbound and outbound traffic**
- **IAM Role defined in the Security Group is different from the IAM Role that is given access in the Network ACLs**

Pregunta 51:

The engineering team at a logistics company has noticed that the Auto Scaling group (ASG) is not terminating an unhealthy Amazon EC2 instance.

As a Solutions Architect, which of the following options would you suggest to troubleshoot the issue? (Select three)

- **A custom health check might have failed. ASG does not terminate instances that are set unhealthy by custom checks**
- **The EC2 instance could be a spot instance type, which cannot be terminated by ASG**
- **The instance has failed the ELB health check status**
- **A user might have updated the configuration of ASG and increased the minimum number of instances forcing ASG to keep all instances alive**
- **The health check grace period for the instance has not expired**
- **The instance maybe in Impaired status**

Pregunta 52:

A social media application is hosted on an EC2 server fleet running behind an Application Load Balancer. The application traffic is fronted by a CloudFront distribution. The engineering team wants to decouple the user authentication process for the application, so that the application servers can just focus on the business logic.

As a Solutions Architect, which of the following solutions would you recommend to the development team so that it requires minimal development effort?

- **Use Cognito Authentication via Cognito User Pools for your CloudFront distribution**
- **Use Cognito Authentication via Cognito Identity Pools for your Application Load Balancer**
- **Use Cognito Authentication via Cognito Identity Pools for your CloudFront distribution**
- **Use Cognito Authentication via Cognito User Pools for your Application Load Balancer**

Pregunta 53:

An IT company is working on a client project to build a Supply Chain Management application. The web-tier of the application runs on an EC2 instance and the database tier is on Amazon RDS MySQL. For beta testing, all the resources are currently deployed in a single Availability Zone. The development team wants to improve application availability before the go-live.

Given that all end users of the web application would be located in the US, which of the following would be the MOST resource-efficient solution?

- **Deploy the web-tier EC2 instances in two regions, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in read replica configuration**
- **Deploy the web-tier EC2 instances in two Availability Zones, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration**
- **Deploy the web-tier EC2 instances in two regions, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration**
- **Deploy the web-tier EC2 instances in two Availability Zones, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in read replica configuration**

Pregunta 54:

An HTTP application is deployed on an Auto Scaling Group, is accessible from an Application Load Balancer that provides HTTPS termination, and accesses a PostgreSQL database managed by RDS.

How should you configure the security groups? (Select three)

- **The security group of the ALB should have an inbound rule from anywhere on port 443(Correcto)**
- **The security group of the EC2 instances should have an inbound rule from the security group of the ALB on port 80**
- **The security group of the ALB should have an inbound rule from anywhere on port 80**
- **The security group of RDS should have an inbound rule from the security group of the EC2 instances in the ASG on port 80**
- **The security group of the EC2 instances should have an inbound rule from the security group of the RDS database on port 5432**
- **The security group of RDS should have an inbound rule from the security group of the EC2 instances in the ASG on port 5432**

Pregunta 55:

A health-care solutions company wants to run their applications on single-tenant hardware to meet regulatory guidelines.

Which of the following is the MOST cost-effective way of isolating their Amazon EC2 instances to a single tenant?

- **Dedicated Instances**
- **On-Demand Instances**
- **Dedicated Hosts**
- **Spot Instances**

Pregunta 56:

A media company is migrating its flagship application from its on-premises data center to AWS for improving the application's read-scaling capability as well as its availability. The existing architecture leverages a Microsoft SQL Server database that sees a heavy read load. The engineering team does a full copy of the production database every 5 hours to populate a dev database. During this period, application users face high latency leading to a bad user experience.

The company is looking at alternate database options and migrating database engines if required. What would you suggest?

- **Leverage Amazon Aurora MySQL with Multi-AZ Aurora Replicas and create the dev database by restoring from the automated backups of Amazon Aurora**
- **Leverage Amazon RDS for MySQL with a Multi-AZ deployment and use the standby instance as the dev database**
- **Leverage Amazon Aurora MySQL with Multi-AZ Aurora Replicas and restore the dev database via mysqldump**
- **Leverage Amazon RDS for SQL server with a Multi-AZ deployment and read replicas. Use the read replica as the dev database**

Pregunta 57:

You would like to mount a network file system on Linux instances, where files will be stored and accessed frequently at first, and then infrequently. What solution is the MOST cost-effective?

- **Glacier Deep Archive**
- **S3 Intelligent Tiering**
- **EFS IA**
- **FSx for Lustre**

Pregunta 58:

An e-commerce company operates multiple AWS accounts and has interconnected these accounts in a hub-and-spoke style using the AWS Transit Gateway. VPCs have been provisioned across these AWS accounts to facilitate network isolation.

Which of the following solutions would reduce both the administrative overhead and the costs while providing shared access to services required by workloads in each of the VPCs?

- **Use Fully meshed VPC Peers**
- **Use VPCs connected with AWS Direct Connect**
- **Build a shared services VPC**
- **Use Transit VPC to reduce cost and share the resources across VPCs**

Pregunta 59:

A company has historically operated only in the `us-east-1` region and stores encrypted data in S3 using SSE-KMS. As part of enhancing its security posture as well as improving the backup and recovery architecture, the company wants to store the encrypted data in S3 that is replicated into the `us-west-1` AWS region. The security policies mandate that the data must be encrypted and decrypted using the same key in both AWS regions.

Which of the following represents the best solution to address these requirements?

- **Create a CloudWatch scheduled rule to invoke a Lambda function to copy the daily data from the source bucket in `us-east-1` region to the destination bucket in `us-west-1` region. Provide AWS KMS key access to the Lambda function for encryption and decryption operations on the data in the source and destination S3 buckets**
- **Create a new S3 bucket in the `us-east-1` region with replication enabled from this new bucket into another bucket in `us-west-1` region. Enable SSE-KMS encryption on the new bucket in `us-east-1` region by using an AWS KMS multi-region key. Copy the existing data from the current S3 bucket in `us-east-1` region into this new S3 bucket in `us-east-1` region**
- **Enable replication for the current bucket in `us-east-1` region into another bucket in `us-west-1` region. Share the existing AWS KMS key from `us-east-1` region to `us-west-1` region**

- **Change the AWS KMS single region key used for the current S3 bucket into an AWS KMS multi-region key.**
Enable S3 batch replication for the existing data in the current bucket in `us-east-1` region into another bucket in `us-west-1` region

Pregunta 60:

A startup has just developed a video backup service hosted on a fleet of EC2 instances. The EC2 instances are behind an Application Load Balancer and the instances are using EBS volumes for storage. The service provides authenticated users the ability to upload videos that are then saved on the EBS volume attached to a given instance. On the first day of the beta launch, users start complaining that they can see only some of the videos in their uploaded videos backup. Every time the users log into the website, they claim to see a different subset of their uploaded videos.

Which of the following is the MOST optimal solution to make sure that users can view all the uploaded videos? (Select two)

- **Write a one time job to copy the videos from all EBS volumes to RDS and then modify the application to use RDS for storing the videos**
- **Write a one time job to copy the videos from all EBS volumes to DynamoDB and then modify the application to use DynamoDB for storing the videos**
- **Write a one time job to copy the videos from all EBS volumes to S3 Glacier Deep Archive and then modify the application to use S3 Glacier Deep Archive for storing the videos**
- **Mount EFS on all EC2 instances. Write a one time job to copy the videos from all EBS volumes to EFS. Modify the application to use EFS for storing the videos**
- **Write a one time job to copy the videos from all EBS volumes to S3 and then modify the application to use Amazon S3 standard for storing the videos**

Pregunta 61:

What is true about RDS Read Replicas encryption?

- **If the master database is unencrypted, the read replicas can be either encrypted or unencrypted**
- **If the master database is encrypted, the read replicas can be either encrypted or unencrypted**
- **If the master database is unencrypted, the read replicas are encrypted**
- **If the master database is encrypted, the read replicas are encrypted**

Pregunta 62:

A retail company wants to share sensitive accounting data that is stored in an Amazon RDS DB instance with an external auditor. The auditor has its own AWS account and needs its own copy of the database.

Which of the following would you recommend to securely share the database with the auditor?

- **Create a snapshot of the database in Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket**
- **Create an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key**
- **Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket**
- **Set up a read replica of the database and configure IAM standard database authentication to grant the auditor access**

Pregunta 63:

Consider the following policy associated with an IAM group containing several users:

```
{
  "Version": "2012-10-17",
  "Id": "EC2TerminationPolicy",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "us-west-1"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "10.200.200.0/24"
        }
      }
    }
  ]
}
```

Which of the following options is correct?

- Users belonging to the IAM group cannot terminate an EC2 instance in the `us-west-1` region when the user's source IP is 10.200.200.200
- Users belonging to the IAM group can terminate an EC2 instance in the `us-west-1` region when the user's source IP is 10.200.200.200
- Users belonging to the IAM group can terminate an EC2 instance in the `us-west-1` region when the EC2 instance's IP address is 10.200.200.200
- Users belonging to the IAM group can terminate an EC2 instance belonging to any region except the `us-west-1` region when the user's source IP is 10.200.200.200

Pregunta 64:

The engineering team at an e-commerce company is working on cost optimizations for EC2 instances. The team wants to manage the workload using a mix of on-demand and spot instances across multiple instance types. They would like to create an Auto Scaling group with a mix of these instances.

Which of the following options would allow the engineering team to provision the instances for this use-case?

- **You can neither use a launch configuration nor a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost**
- **You can only use a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost**
- **You can use a launch configuration or a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost**
- **You can only use a launch configuration to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost**

Pregunta 65:

A company is developing a healthcare application that cannot afford any downtime for database write operations. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution using Amazon Aurora.

Which of the following options would you recommend?

- **Set up an Aurora multi-master DB cluster**
- **Set up an Aurora provisioned DB cluster**
- **Set up an Aurora Global Database cluster**
- **Set up an Aurora serverless DB cluster**