



Amazon

SAA-C02 Exam

Amazon Associate

Questions & Answers

(Full Version)

Thank you for Purchasing SAA-C02 Exam

Product Questions: 587

Topic 1, Exam Pool A

Question: 1

A company has a service that produces event data

a. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solutions architect accomplish this?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Answer: A

Explanation:

Question: 2

A company currently has 250 TB of backup files stored in Amazon S3 in a vendor's proprietary format. Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversion.

What should a solutions architect do to accomplish this?

- A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.
- B. Install the conversion software onto an on-premises virtual machine. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.
- C. Use AWS Snowball Edge devices to export the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball Edge devices.

D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

Answer: D

Explanation:

Question: 3

A company must migrate 20 TB of data from a data centre to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use AWS DataSync
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration

Answer: A

Explanation:

Question: 4

A solutions architect must create a highly available bastion host architecture. The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain. What should the solutions architect do to meet these requirements?

- A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.
- B. Create a Network Load Balancer backed by a Spot Fleet with instances in a partition placement group.
- C. Create a Network Load Balancer backed by the existing servers in different Availability Zones as the target.
- D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target

Answer: D

Explanation:

Question: 5

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest.

Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

- A. Deploy AWS Certificate Manager to generate certificates Use the certificates to encrypt the database volume
- B. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes
- C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes.
- D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes

Answer: D

Explanation:

Question: 6

A company is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in Amazon RDS MySQL Multi-AZ DB instances. The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks.

What should a solutions architect recommend?

- A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Configure the EC2 instance iptables rules to drop suspicious web traffic. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Move DB instances to the same subnets that EC2 instances are located in. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.
- D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Configure the Auto Scaling group to automatically create new DB instances under heavy traffic. Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

Answer: C

Explanation:

Question: 7

A company's packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution^ but wants to further reduce data transfer costs. The company cannot modify the application's source code. What should a solutions architect do to reduce costs?

- A. Use Lambda@Edge to compress the files as they are sent to users.
- B. Enable Amazon S3 Transfer Acceleration to reduce the response times
- C. Enable caching on the CloudFront distribution to store generated files at the edge.
- D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users

Answer: C

Explanation:

Question: 8

A company is building a mobile app on AWS. The company wants to expand its reach to millions of users. The company needs to build a platform so that authorized users can watch the company's content on their mobile devices.

What should a solutions architect recommend to meet these requirements?

- A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.
- B. Set up IPsec VPN between the mobile app and the AWS environment to stream content.
- C. Use Amazon CloudFront to provide signed URLs to stream content.
- D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

Answer: C

Explanation:

Question: 9

A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises file-based applications. The data files are stored in an Amazon S3 bucket that has read-only permissions for each clinic.

What should a solutions architect recommend to meet these requirements?

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic.
- B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.
- C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises at each clinic.
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on-premises servers.

Answer: A

Explanation:

Question: 10

A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an Application Load Balancer (ALB). The current

failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region

What should a solutions architect do to automate the failover process?

- A. Enable an ALB health check
- B. Enable an Amazon Route 53 health check
- C. Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint.
- D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server

Answer: B

Explanation:

Question: 11

A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.

The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application to asynchronously dispatch requests to the different application tiers.

What should the solutions architect do to meet these requirements?

- A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.
- B. Create an AWS Step Functions workflow Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete
- C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received
- D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions Use one subscription with the application to generate the thumbnail after the image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.

Answer: A

Explanation:

Question: 12

A company is using AWS Key Management Service (AWS KMS) customer master keys (CMKs) to encrypt AWS Lambda environment variables A solutions architect needs to ensure that the required permissions are in place to decrypt and use the environment variables.

Which steps must the solutions architect take to implement the correct permissions? (Select TWO.)

- A. Add AWS KMS permissions in the Lambda resource policy
- B. Add AWS KMS permissions in the Lambda execution role

- C. Add AWS KMS permissions in the Lambda function policy.
- D. Allow the Lambda execution role in the AWS KMS key policy
- E. Allow the Lambda resource policy in the AWS KMS key policy.

Answer: BC

Explanation:

Question: 13

A company operates a website on Amazon EC2 Linux instances. Some of the instances are failing. Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this.

What should a solutions architect recommend?

- A. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
- B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch.
- C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.
- D. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch.

Answer: A

Explanation:

Question: 14

A company needs a storage solution for an application that runs on a high performance computing (HPC) cluster. The cluster is hosted on AWS Fargate for Amazon Elastic Container Service (Amazon ECS). The company needs a mountable file system that provides concurrent access to files while delivering hundreds of GBps of throughput at sub-millisecond latencies.

Which solution meets these requirements?

- A. Create an Amazon FSx for Lustre file share for the application data. Create an IAM role that allows Fargate to access the FSx for Lustre file share.
- B. Create an Amazon Elastic File System (Amazon EFS) file share for the application data. Create an IAM role that allows Fargate to access the EFS file share.
- C. Create an Amazon S3 bucket for the application data. Create an S3 bucket policy that allows Fargate to access the S3 bucket.
- D. Create an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io2) volume for the application data. Create an IAM role that allows Fargate to access the volume.

Answer: A

Explanation:

Question: 15

A company runs an application on Amazon EC2 instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that is highly available across the Region. Which solution should be implemented to ensure that there are no disruptions to internet connectivity?

- A. Deploy a NAT instance in a private subnet of each Availability Zone.
- B. Deploy a NAT gateway in a public subnet of each Availability Zone.
- C. Deploy a transit gateway in a private subnet of each Availability Zone.
- D. Deploy an internet gateway in a public subnet of each Availability Zone.

Answer: B

Explanation:

Question: 16

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database. What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database.
- B. Update the application to read from the Multi-AZ standby instance.
- C. Create a read replica and modify the application to use the appropriate endpoint.
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Answer: C

Explanation:

Question: 17

An administrator of a large company wants to monitor for and prevent any cryptocurrency-related attacks on the company's AWS accounts. Which AWS service can the administrator use to protect the company against attacks?

- A. Amazon Cognito
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. Amazon Macie

Answer: B

Explanation:

Question: 18

A company has applications that are deployed in multiple AWS Regions. The applications use an architecture that is based on Amazon EC2, Amazon Elastic Block Store (Amazon EBS), Amazon Elastic File System (Amazon EFS), and Amazon DynamoDB.

The company lacks a mechanism for centralized data backup. A solutions architect must centralize data backup with the least possible operational effort.

What should the solutions architect do to meet these requirements?

- A. Tag all resources by project. Use AWS Systems Manager to set up snapshots by project and set DynamoDB incremental backups.
- B. Tag all resources by project. Create backup plans in AWS Backup to back up the data by tag name according to each project's needs.
- C. Tag all resources by project. Create an AWS Lambda function to run on schedule and take snapshots of each EC2 instance, EBS volume, and EFS file system by project. Configure the function to invoke DynamoDB on-demand backup.
- D. Use AWS CloudFormation to create a template for every new project so that all resources can be recreated at any time. Set the template to take daily snapshots of each EC2 instance, EBS volume, and EFS file system. Set the template to use DynamoDB on-demand backup for daily backups.

Answer: B

Explanation:

Question: 19

A solutions architect needs to design a resilient solution for Windows users' home directories. The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company's Active Directory.

Which storage solution meets these requirements?

- A. Configure Amazon S3 to store the users' home directories. Join Amazon S3 to Active Directory.
- B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server. Join Amazon FSx to Active Directory.
- C. Configure Amazon Elastic File System (Amazon EFS) for the users' home directories. Configure AWS Single Sign-On with Active Directory.
- D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users' home directories. Configure AWS Single Sign-On with Active Directory.

Answer: B

Explanation:

Question: 20

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

- A. Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set.

- B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-aci header set to private.
- C. Update the bucket policy to deny if the PutObject does not have an awsSecureTransport header set to true
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

Answer: D

Explanation:

Question: 21

A company's database is hosted on an Amazon Aurora MySQL DB cluster in the us-east-1 Region. The database is 4 TB in size. The company needs to expand its disaster recovery strategy to the us-west-2 Region. The company must have the ability to fail over to us-west-2 with a recovery time objective (RTO) of 15 minutes.

What should a solutions architect recommend to meet these requirements?

- A. Create a Multi-Region Aurora MySQL DB cluster in us-east-1 and us-west-2. Use an Amazon Route 53 health check to monitor us-east-1 and fail over to us-west-2 upon failure.
- B. Take a snapshot of the DB cluster in us-east-1. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to copy the snapshot to us-west-2 and restore the snapshot in us-west-2 when failure is detected.
- C. Create an AWS CloudFormation script to create another Aurora MySQL DB cluster in us-west-2 in case of failure. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to deploy the AWS CloudFormation stack in us-west-2 when failure is detected.
- D. Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to promote the DB cluster in us-west-2 when failure is detected.

Answer: B

Explanation:

Question: 22

A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However, the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds.

How can this issue be addressed?

- A. Reduce the threshold for CPU utilization in the Auto Scaling group
- B. Replace the Application Load Balancer with a Network Load Balancer.
- C. Add read replicas for the RDS instances and direct read traffic to the replica
- D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance

Answer: C

Explanation:

Question: 23

A solutions architect needs to design a network that will allow multiple Amazon EC2 instances to access a common data source used for mission-critical data that can be accessed by all the EC2 instances simultaneously. The solution must be highly scalable, easy to implement, and support the NFS protocol

Which solution meets these requirements?

- A. Create an Amazon EFS file system Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target
- B. Create an additional EC2 instance and configure it as a file server Create a security group that allows communication between the instances and apply that to the additional instance.
- C. Create an Amazon S3 bucket with the appropriate permissions Create a role in AWS IAM that grants the correct permissions to the S3 bucket. Attach the role to the EC2 instances that need access to the data
- D. Create an Amazon EBS volume with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the EBS volume. Attach the role to the EC2 instances that need access to the data.

Answer: A

Explanation:

Question: 24

A disaster response team is using drones to collect images of recent storm damage. The response team's laptops lack the storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.

What should a solutions architect recommend'?

- A. Use AWS Snowball Edge devices to process and store the images
- B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
- C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images
- D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

Answer: A

Explanation:

Question: 25

A company has an ecommerce application that stores data in an on-premises SQL database. The company has decided to migrate this database to AWS. However, as part of the migration, the company wants to find a way to attain sub-millisecond responses to common read requests. A solutions architect knows that the increase in speed is paramount and that a small percentage of stale data returned in the database reads is acceptable.

What should the solutions architect recommend'?

- A. Build Amazon RDS read replicas.
- B. Build the database as a larger instance type.
- C. Build a database cache using Amazon ElastiCache
- D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

Answer: C

Explanation:

Question: 26

A solutions architect must provide a fully managed replacement for an on-premises solution that allows employees and partners to exchange files. The solution must be easily accessible to employees connecting from on-premises systems, remote employees, and external partners.

Which solution meets these requirements?

- A. Use AWS Transfer for SFTP to transfer files into and out of Amazon S3.
- B. Use AWS Snowball Edge for local storage and large-scale data transfers.
- C. Use Amazon FSx to store and transfer files to make them available remotely.
- D. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.

Answer: A

Explanation:

Question: 27

A company has an application that uses Amazon Elastic File System (Amazon EFS) to store data. The files are 1 GB in size or larger and are accessed often only for the first few days after creation. The application data is shared across a cluster of Linux servers. The company wants to reduce storage costs for the application.

What should a solutions architect do to meet these requirements?

- A. Implement Amazon FSx and mount the network drive on each server.
- B. Move the files from Amazon EFS and store them locally on each Amazon EC2 instance.
- C. Configure a lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7

days.

D. Move the files to Amazon S3 with S3 Lifecycle policies enabled. Rewrite the application to support mounting the S3 bucket

Answer: C

Explanation:

Question: 28

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group
- B. Use a target tracking policy to dynamically scale the Auto Scaling group
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group

Answer: B

Explanation:

Question: 29

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF.

How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
- B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
- C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
- D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Answer: B

Explanation:

Question: 30

A company is hosting an application in its own data center. The application uses Amazon S3 for data storage. The application transfers several hundred terabytes of data every month to and from

Amazon S3 The company needs to minimize the cost of this data transfer
Which solution meets this requirement?

- A. Establish an AWS Direct Connect connection between the AWS Region in use and the company's data center Route traffic to Amazon S3 over the Direct Connect connection
- B. Establish an AWS Site-to-Site VPN connection between the company's data center and a VPC in the AWS Region in use. Create a VPC endpoint for Amazon S3 in the VPC. Route traffic to Amazon S3 over the VPN connection to the S3 endpoint.
- C. Create an AWS Storage Gateway file gateway Deploy the software appliance in the company's data center Configure the application to use the file gateway to store and retrieve files
- D. Create an FTPS server by using AWS Transfer Family. Configure the application to use the FTPS server to store and retrieve files

Answer: C

Explanation:

Question: 31

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements all existing and new data in this database must be encrypted.

How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled Move all the data to Amazon S3 Delete the RDS instance
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled Promote the read replica to master and switch the application over to the new master Delete the old RDS instance

Answer: C

Explanation:

Question: 32

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    },
    {
      "Sid": "2",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
      }
    }
  ]
}

{
  "Sid": "2",
  "Effect": "Deny",
  "Action": [
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource": "*",
  "Condition": {
    "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
  }
}

```

What are the effective IAM permissions of this policy for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
- B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
- C. Group members are allowed the ec2 StopInstances and ec2. TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA) Group members are permitted any other Amazon EC2 action.
- D. Group members are allowed the ec2 StopInstances and ec2. Terminateinstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA) Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Answer: D

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/APIReference/ec2-api-permissions.html>

By default, AWS Identity and Access Management (IAM) users don't have permission to create or modify Amazon EC2 resources, or perform tasks using the Amazon EC2 API. To allow IAM users to create or modify resources and perform tasks, you must create IAM policies that grant IAM users permissions for the specific resources and API actions they'll need to use, and then attach those policies to the IAM users or groups that require those permissions.

Question: 33

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance. Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

Answer: B

Explanation:

Question: 34

A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.

Which solution should a solutions architect recommend to keep the data private?

- A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.
- B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.
- C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.
- D. Deploy an AWS Storage Gateway file gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

Answer: A

Explanation:

Question: 35

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "10.100.100.0/24"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    }
  ]
}
```

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254

Answer: A

Explanation:

Question: 36

A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly.

Which actions should a solutions architect take to meet this requirement? (Select TWO.)

- A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key
- B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
- C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key
- D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue. Set the message attribute to use the payment ID
- E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Answer: AE

Explanation:

Question: 37

A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.

Which solution meets these requirements?

- A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.
- D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

Answer: B

Explanation:

Question: 38

A solutions architect must design a database solution for a high-traffic ecommerce web application. The database stores customer profiles and shopping cart information. The database must support a peak load of several million requests each second and deliver responses in milliseconds. The operational overhead for managing and scaling the database must be minimized. Which database solution should the solutions architect recommend?

- A. Amazon Aurora
- B. Amazon DynamoDB
- C. Amazon RDS
- D. Amazon Redshift

Answer: B

Explanation:

Question: 39

A company wants to run a hybrid workload for data processing. The data needs to be accessed by on-premises applications for local data processing using an NFS protocol and must also be accessible from the AWS Cloud for further analytics and batch processing. Which solution will meet these requirements?

- A. Use an AWS Storage Gateway file gateway to provide file storage to AWS; then perform analytics on this data in the AWS Cloud.
- B. Use an AWS Storage Gateway tape gateway to copy the backup of the local data to AWS; then perform analytics on this data in the AWS Cloud.
- C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.
- D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS Cloud, then perform analytics on this data in the cloud.

Answer: A

Explanation:

Question: 40

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store process, and delete the messages., respectively.
- B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
- C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
- D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process, integrate the sender application to write to the SNS topic.

Answer: C

Explanation:

Question: 41

A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.

What is the MOST cost-effective storage solution for this situation?

- A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
- B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
- C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
- D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Answer: D

Explanation:

Question: 42

A company's website hosted on Amazon EC2 instances processes classified data stored in Amazon S3. Due to security concerns, the company requires a private and secure connection between its EC2 resources and Amazon S3.

Which solution meets these requirements?

- A. Set up S3 bucket policies to allow access from a VPC endpoint.
- B. Set up an IAM policy to grant read-write access to the S3 bucket.
- C. Set up a NAT gateway to access resources outside the private subnet.
- D. Set up an access key ID and a secret access key to access the S3 bucket.

Answer: A

Explanation:

Question: 43

A company has a custom application running on an Amazon EC2 instance that

- Reads a large amount of data from Amazon S3
- Performs a multi-stage analysis.

Writes the results to Amazon DynamoDB

The application writes a significant number of large, temporary files during the multi-stage analysis.

The process performance depends on the temporary storage performance. What would be the

fastest storage option for holding the temporary files?

- A. Multiple Amazon S3 buckets with Transfer Acceleration for storage
- B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization
- C. Multiple Amazon EFS volumes using the Network File System version 4.1 (NFSv4.1) protocol
- D. Multiple instance store volumes with software RAID 0.

Answer: A

Explanation:

Question: 44

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

- A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
- C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts
- D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account

Answer: C

Explanation:

Question: 45

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO.)

- A. Add AWS Shield
- B. Add Aurora Replicas.
- C. Add AWS Direct Connect
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Answer: BE

Explanation:

Question: 46

A company has developed a microservices application. It uses a client-facing API with Amazon API Gateway and multiple internal services hosted on Amazon EC2 instances to process user requests. The API is designed to support unpredictable surges in traffic, but internal services may become overwhelmed and unresponsive for a period of time during surges. A solutions architect needs to design a more reliable solution that reduces errors when internal services become unresponsive or unavailable.

Which solution meets these requirements?

- A. Use AWS Auto Scaling to scale up internal services when there is a surge in traffic.
- B. Use different Availability Zones to host internal services. Send a notification to a system administrator when an internal service becomes unresponsive.
- C. Use an Elastic Load Balancer to distribute the traffic between internal services. Configure Amazon CloudWatch metrics to monitor traffic to internal services.
- D. Use Amazon Simple Queue Service (Amazon SQS) to store user requests as they arrive. Change the internal services to retrieve the requests from the queue for processing.

Answer: D

Explanation:

Question: 47

A company is designing a new application that runs in a VPC on Amazon EC2 instances. The application stores data in Amazon S3 and uses Amazon DynamoDB as its database. For compliance reasons, the company prohibits all traffic between the EC2 instances and other AWS services from passing over the public internet.

What can a solutions architect do to meet this requirement?

- A. Configure gateway VPC endpoints to Amazon S3 and DynamoDB.
- B. Configure interface VPC endpoints to Amazon S3 and DynamoDB.
- C. Configure a gateway VPC endpoint to Amazon S3. Configure an interface VPC endpoint to DynamoDB.
- D. Configure a gateway VPC endpoint to DynamoDB. Configure an interface VPC endpoint to Amazon S3.

Answer: A

Explanation:

Question: 48

A company needs to implement a relational database with a multi-Region disaster recovery. Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables

- C. Amazon RDS for MySQL with Multi-AZ enabled
- D. Amazon RDS for MySQL with a cross-Region snapshot copy

Answer: A

Explanation:

Question: 49

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon DynamoDB
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balancers

Answer: A

Explanation:

Question: 50

A company is developing a new online gaming application. The application will run on Amazon EC2 instances in multiple AWS Regions and will have a high number of globally distributed users. A solutions architect must design the application to optimize network latency for the users.

Which actions should the solutions architect take to meet these requirements? (Select TWO.)

- A. Configure AWS Global Accelerator. Create Regional endpoint groups in each Region where an EC2 fleet is hosted.
- B. Create a content delivery network (CDN) by using Amazon CloudFront. Enable caching for static and dynamic content, and specify a high expiration period.
- C. Integrate AWS Client VPN into the application. Instruct users to select which Region is closest to them after they launch the application. Establish a VPN connection to that Region.
- D. Create an Amazon Route 53 weighted routing policy. Configure the routing policy to give the highest weight to the EC2 instances in the Region that has the largest number of users.
- E. Configure an Amazon API Gateway endpoint in each Region where an EC2 fleet is hosted. Instruct users to select which Region is closest to them after they launch the application. Use the API Gateway endpoint that is closest to them.

Answer: AB

Explanation:

Question: 51

A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application. What should the solutions architect do to meet this requirement?

- A. Add an Amazon Inspector agent to the ALB
- B. Configure Amazon GuardDuty to prevent attacks.
- C. Enable AWS Shield Advanced to prevent attacks.
- D. Configure Amazon GuardDuty to monitor the ALB

Answer: C

Explanation:

Question: 52

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API. Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3
- B. Use Amazon API Gateway with AWS Lambda
- C. Use Amazon QuickSight with Amazon Redshift.
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Answer: D

Explanation:

Question: 53

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images. Which method is the MOST cost-effective for hosting the website?

- A. Containerize the website and host it in AWS Fargate.
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

Answer: B

Explanation:

Question: 54

A company hosts its multi-tier, public web application in the AWS Cloud. The web application runs on Amazon EC2 instances and its database runs on Amazon RDS. The company is anticipating a large increase in sales during an upcoming holiday weekend. A solutions architect needs to build a solution to analyze the performance of the web application with a granularity of no more than 2 minutes. What should the solutions architect do to meet this requirement?

- A. Send Amazon CloudWatch logs to Amazon Redshift. Use Amazon QuickSight to perform further analysis.
- B. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.
- C. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform further analysis.
- D. Send EC2 logs to Amazon S3. Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.

Answer: B

Explanation:

Question: 55

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure. Which combination of actions should the solutions architect take to accomplish this? (Select TWO.)

- A. Migrate the PostgreSQL database to Amazon Aurora.
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Answer: CD

Explanation:

Question: 56

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.

What should a solutions architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an associated Elastic IP address.
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address.
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer.

Answer: A

Explanation:

Question: 57

A manufacturing company has machine sensors that upload csv files to an Amazon S3 bucket. These csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports.

The images become irrelevant after 1 month, but the csv files must be kept to train machine learning (ML) models twice a year. The ML trainings and audits are planned weeks in advance.

Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO)

- A. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.
- B. Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucket. Invoke the Lambda function when a csv file is uploaded.
- C. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the csv files from S3 Standard to S3 Glacier 1 day after they are uploaded. Expire the image files after 30 days.
- D. Create S3 Lifecycle rules for csv files and image files in the S3 bucket. Transition the csv files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 1 day after they are uploaded. Expire the image files after 30 days.
- E. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).

Answer: BD

Explanation:

Question: 58

A company's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.

Which combination of steps should the solutions architect take? (Select TWO.)

- A. Use Amazon Kinesis Data Firehose to ingest the data.
- B. Use AWS Lambda with AWS Step Functions to process the data.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data.
- D. Use Amazon EC2 instances in an Auto Scaling group to process the data.
- E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Answer: A,B

Explanation:

Question: 59

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow

Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution
- B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register the instances with the same ALB using cross-Region VPC peering.
- D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Answer: A

Explanation:

Question: 60

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently. What should a solutions architect do to meet these requirements when configuring the logs?

- A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.
- B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
- C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
- D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Answer: A

Explanation:

Question: 61

A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead.

What should the solutions architect do to meet these requirements?

- A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.

- B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
- C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
- D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Answer: B

Explanation:

Question: 62

A company needs to connect its on-premises data center network to a new VPC. The data center network has a 100 Mbps symmetrical internet connection. An application that is running on premises will transfer multiple gigabytes of data each day. The application will use an Amazon Kinesis Data Firehose delivery stream for processing.

What should a solutions architect recommend for maximum performance?

- A. Create a VPC peering connection between the on-premises network and the VPC. Configure routing for the on-premises network to use the VPC peering connection.
- B. Procure an AWS Snowball Edge Storage Optimized device. After several days' worth of data has accumulated, copy the data to the device and ship the device to AWS for expedited transfer to Kinesis Data Firehose. Repeat as needed.
- C. Create an AWS Site-to-Site VPN connection between the on-premises network and the VPC. Configure BGP routing between the customer gateway and the virtual private gateway. Use the VPN connection to send the data from on premises to Kinesis Data Firehose.
- D. Use AWS PrivateLink to create an interface VPC endpoint for Kinesis Data Firehose in the VPC. Set up a 1 Gbps AWS Direct Connect connection between the on-premises network and AWS. Use the PrivateLink endpoint to send the data from on premises to Kinesis Data Firehose.

Answer: D

Explanation:

Question: 63

A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company wants to deploy the application across multiple AWS Regions to provide Regional failover capabilities.

What should a solutions architect do to route traffic to multiple Regions?

- A. Configure Amazon Route 53 health checks for each Region. Use an active-active failover configuration.
- B. Create an Amazon CloudFront distribution with an origin for each Region. Use CloudFront health checks to route traffic.
- C. Create an AWS Transit Gateway. Attach the transit gateway to the API Gateway endpoint in each Region. Configure the transit gateway to route requests.
- D. Use AWS Global Accelerator to create an accelerator with endpoints in each Region. Allow Global

Accelerator to automatically monitor the health of endpoints and route requests.

Answer: A

Explanation:

Question: 64

A company is planning to migrate a TCP-based application into the company's VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company's data centre. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS.

What should a solutions architect recommend to meet this requirement?

- A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
- B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
- C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
- D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

Answer: A

Explanation:

Question: 65

A company is automating an order management application. The company's development team has decided to use SFTP to transfer and store the business-critical information files. The files must be encrypted and must be highly available. The files also must be automatically deleted a month after they are created.

Which solution meets these requirements with the LEAST operational overhead?

- A. Configure an Amazon S3 bucket with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the S3 bucket. Apply an AWS Transfer for SFTP file retention policy to delete the files after a month.
- B. Install an SFTP service on an Amazon EC2 instance. Mount an Amazon Elastic File System (Amazon EFS) file share on the EC2 instance. Enable cron to delete the files after a month.
- C. Configure an Amazon Elastic File System (Amazon EFS) file system with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the EFS file system. Apply an EFS lifecycle policy to automatically delete the files after a month.
- D. Configure an Amazon S3 bucket with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the S3 bucket. Apply S3 Lifecycle rules to automatically delete the files after a month.

Answer: D

Explanation:

Question: 66

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

Which change to the network architecture should a solutions architect recommend to meet this requirement?"

- A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.
- B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.
- C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets
- D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Answer: C

Explanation:

Question: 67

A company processes large amounts of data

a. The output data is stored in Amazon S3 Standard storage in an S3 bucket, where it is analyzed for 1 month. The data must remain immediately accessible after the 1-month analysis period.

Which storage solution meets these requirements MOST cost-effectively?

- A. Configure an S3 Lifecycle policy to transition the objects to S3 Glacier after 30 days.
- B. Configure S3 Intelligent-Tiering to transition the objects to S3 Glacier after 30 days.
- C. Configure an S3 Lifecycle policy to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Configure an S3 Lifecycle policy to delete the objects after 30 days. Enable versioning on the S3 bucket so that deleted objects can still be immediately restored as needed.

Answer: B

Explanation:

Question: 68

A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to

consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.

Which solution meets these requirements?

- A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.
- D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

Answer: C

Explanation:

Question: 69

A company hosts an application on AWS. The application interacts with an Amazon DynamoDB table that has 10 read capacity units (RCUs). Data from Amazon CloudWatch alarms shows that throttling is occurring on read requests to the DynamoDB table. The company needs to prevent this issue from happening in the future as the application continues to grow.

What should a solutions architect recommend to meet these requirements?

- A. Add an Elastic Load Balancer in front of the DynamoDB table.
- B. Change the RCUs for the DynamoDB table to 20.
- C. Provision 20 write capacity units (WCUs) for the DynamoDB table to offset the throttling on read requests.
- D. Enable auto scaling for the DynamoDB table.

Answer: D

Explanation:

Question: 70

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

- A. Read replicas
- B. Manual snapshots

- C. Automated backups
- D. Multi-AZ deployments

Answer: C

Explanation:

Question: 71

A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs to share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses a customer managed customer master key (CMK) to encrypt EBS volume snapshots.

What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

- A. Make the encrypted AMI and snapshots publicly available. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key
- B. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.
- C. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the CMK's key policy to trust a new CMK that is owned by the MSP Partner for encryption.
- D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account. Encrypt the S3 bucket with a CMK that is owned by the MSP Partner. Copy and launch the AMI in the MSP Partner's AWS account.

Answer: B

Explanation:

Question: 72

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs'?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication
- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication
- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Answer: C

Explanation:

Question: 73

A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website. The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads. Which combination of actions should the solutions architect take to meet these requirements? (Select TWO.)

- A. Configure the application to upload images to S3 Glacier.
- B. Configure the web server to upload the original images to Amazon S3.
- C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL.
- D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image.
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

Answer: DE

Explanation:

Question: 74

A company is developing a serverless web application that gives users the ability to interact with real-time analytics from online games. The data from the games must be streamed in real time. The company needs a durable, low-latency database option for user data.
a. The company does not know how many users will use the application. Any design considerations must provide response times of single-digit milliseconds as the application scales.
Which combination of AWS services will meet these requirements? (Select TWO.)

- A. Amazon CloudFront
- B. Amazon DynamoDB
- C. Amazon Kinesis
- D. Amazon RDS
- E. AWS Global Accelerator

Answer: B, C

Explanation:

Question: 75

A solutions architect must transfer 750 TB of data from an on-premises network-attached file system to Amazon S3 Glacier. The migration must not saturate the on-premises 10 Mbps internet connection.

Which solution will meet these requirements?

- A. Create an AWS Site-to-Site VPN tunnel to an S3 bucket Transfer the files directly by using the AWS CLI.
- B. Order 10 AWS Snowball Edge Storage Optimized devices, and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to an S3 bucket, and copy the files directly. Create an S3 Lifecycle policy to transition the S3 objects to S3 Glacier.
- D. Order 10 AWS Snowball Edge Storage Optimized devices, and select an S3 bucket as the destination. Create an S3 Lifecycle policy to transition the S3 objects to S3 Glacier.

Answer: D

Explanation:

Question: 76

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However many of the web service clients can only reach IP addresses whitelisted on their firewalls.

What should a solutions architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address
- B. An Application Load Balancer with an associated Elastic IP address.
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer.

Answer: A

Explanation:

Question: 77

A solutions architect is designing the architecture for a new web application. The application will run on AWS Fargate containers with an Application Load Balancer (ALB) and an Amazon Aurora PostgreSQL database. The web application will perform primarily read queries against the database. What should the solutions architect do to ensure that the website can scale with increasing traffic? (Select TWO.)

- A. Enable auto scaling on the ALB to scale the load balancer horizontally.
- B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.
- C. Enable cross-zone load balancing on the ALB to distribute the load evenly across containers in all Availability Zones.
- D. Configure an Amazon Elastic Container Service (Amazon ECS) cluster in each Availability Zone to distribute the load across multiple Availability Zones.
- E. Configure Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling with a target tracking scaling policy that is based on CPU utilization.

Answer: AB

Explanation:

Question: 78

A company wants to run an in-memory database for a latency-sensitive application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and requires high network throughput. A solutions architect needs to provide a cost-effective network design that minimizes data transfer charges.

Which solution meets these requirements?

- A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.
- B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.
- C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.
- D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

Answer: A

Explanation:

Question: 79

A company has a customer relationship management (CRM) application that stores data in an Amazon RDS DB instance that runs Microsoft SQL Server. The company's IT staff has administrative access to the database. The database contains sensitive data.

- a. The company wants to ensure that the data is not accessible to the IT staff and that only authorized personnel can view the data.

What should a solutions architect do to secure the data?

- A. Use client-side encryption with an Amazon RDS managed key.
- B. Use client-side encryption with an AWS Key Management Service (AWS KMS) customer managed key.
- C. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) default encryption key.
- D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

Answer: D

Explanation:

Question: 80

A company is running a web application on Amazon EC2 instances in an Auto Scaling group. The application uses a database that runs on an Amazon RDS for PostgreSQL DB instance. The application performs slowly as traffic increases, and the database experiences a heavy read load during periods of high traffic.

Which actions should a solutions architect take to resolve these performance issues? (Select TWO.)

- A. Enable auto scaling for the DB instance.
- B. Create a read replica for the DB instance. Configure the application to send read traffic to the read replica.
- C. Enable Multi-AZ for the DB instance. Configure the application to send read traffic to the standby DB instance.
- D. Create an Amazon ElastiCache cluster. Configure the application to cache query results in the ElastiCache cluster.
- E. Configure the Auto Scaling group subnets to ensure that the EC2 instances are provisioned in the same Availability Zone as the DB instance.

Answer: B, D

Explanation:

Question: 81

A company is running an application on Amazon EC2 instances. Traffic to the workload increases substantially during business hours and decreases afterward. The CPU utilization of an EC2 instance is a strong indicator of end-user demand on the application. The company has configured an Auto Scaling group to have a minimum group size of 2 EC2 instances and a maximum group size of 10 EC2 instances.

The company is concerned that the current scaling policy that is associated with the Auto Scaling group might not be correct. The company must avoid over-provisioning EC2 instances and incurring unnecessary costs.

What should a solutions architect recommend to meet these requirements?

- A. Configure Amazon EC2 Auto Scaling to use a scheduled scaling plan and launch an additional 8 EC2 instances during business hours.
- B. Configure AWS Auto Scaling to use a scaling plan that enables predictive scaling. Configure predictive scaling with a scaling mode of forecast and scale, and to enforce the maximum capacity setting during scaling.
- C. Configure a step scaling policy to add 4 EC2 instances at 50% CPU utilization and add another 4 EC2 instances at 90% CPU utilization. Configure scale-in policies to perform the reverse and remove EC2 instances based on the two values.
- D. Configure AWS Auto Scaling to have a desired capacity of 5 EC2 instances, and disable any existing scaling policies. Monitor the CPU utilization metric for 1 week. Then create dynamic scaling policies that are based on the observed values.

Answer: B

Explanation:

Question: 82

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.

The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data.

a. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.

What should a solutions architect do to improve the performance of the data tier?

- A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
- B. Migrate from Amazon RDS to Amazon Elasticsearch Service (Amazon ES) with Kibana.
- C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.
- D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

Answer: D

Explanation:

Question: 83

A company captures ordered clickstream data from multiple websites and uses batch processing to analyze the data.

a. The company receives 100 million event records, all approximately 1 KB in size, each day. The company loads the data into Amazon Redshift each night, and business analysts consume the data.

The company wants to move toward near-real-time data processing for timely insights. The solution should process the streaming data while requiring the least possible operational overhead.

Which combination of AWS services will meet these requirements MOST cost-effectively? (Select TWO.)

- A. Amazon EC2
- B. AWS Batch
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer: BC

Explanation:

Question: 84

A company has been running a web application with an Oracle relational database in an on-premises data center for the past 15 years. The company must migrate the database to AWS. The company needs to reduce operational overhead without having to modify the application's code.

Which solution meets these requirements?

- A. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon RDS.
- B. servers.
- C. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon DynamoDB.
- D. Use an AWS Snowball Edge Storage Optimized device to migrate the data from Oracle to Amazon Aurora.

Answer: C

Explanation:

Question: 85

A company has three VPCs named Development, Testing and Production in the us-east-1 Region. The three VPCs need to be connected to an on-premises data center and are designed to be separate to maintain security and prevent any resource sharing. A solutions architect needs to find a scalable and secure solution.

What should the solutions architect recommend?

- A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.
- B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.
- C. Connect VPN connections from all the VPCs to a VPN in the Production VPC. Use a VPN connection from the Production VPC back to the data center.
- D. Create a new VPC called Network. Within the Network VPC, create an AWS Transit Gateway with an AWS Direct Connect connection back to the data center. Attach all the other VPCs to the Network VPC.

Answer: D

Explanation:

Question: 86

A solutions architect is redesigning a monolithic application to be a loosely coupled application composed of two microservices: Microservice A and Microservice B. Microservice A places messages in an Amazon Simple Queue Service (Amazon SQS) queue for Microservice B to consume. When Microservice B fails to process a message after four retries, the message needs to be removed from the queue and stored for further investigation.

What should the solutions architect do to meet these requirements?

- A. Create an SQS dead-letter queue. Microservice B adds failed messages to that queue after it receives and fails to process the message four times.
- B. Create an SQS dead-letter queue. Configure the main SQS queue to deliver messages to the dead-letter queue after the message has been received four times.
- C. Create an SQS queue for failed messages. Microservice A adds failed messages to that queue after Microservice B receives and fails to process the message four times.
- D. Create an SQS queue for failed messages. Configure the SQS queue for failed messages to pull messages from the main SQS queue after the original message has been received four times.

Answer: B

Explanation:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html#sqs-dead-letter-queues-how-they-work>

Question: 87

A solution architect at a company is designing the architecture for a two-tiered web application. The web application is composed of an internet facing application load balancer that forwards traffic to an auto scaling group of amazon EC2 instances. The EC2 instances must be able to access a database that runs on Amazon RDS.

The company has requested a defence-in-depth approach to the network layout. The company does not want to rely solely on security groups or network ACLs. Only the minimum resources that are necessary should be routable from the internet.

Which network design should the solutions architect recommend to meet these requirements?

- A. Place the ALB, EC2 instances and RDS database in private subnets.
- B. Place the ALB in public subnets. Place the EC2 instances and RDS database in private subnets
- C. Place the ALB and EC2 instances in public subnets. Place the RDS database in private subnets
- D. Place the ALB outside the VPC. Place the EC2 instances and RDS database in private subnets.

Answer: C

Explanation:

Question: 88

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models.

Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

Which storage solution meets these requirements MOST cost-effectively?

- A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
- C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Answer: B

Explanation:

Question: 89

A company is migrating a large, mission-critical database to AWS. A solutions architect has decided to use an Amazon RDS for MySQL Multi-AZ DB instance that is deployed with 80,000 Provisioned IOPS for storage. The solutions architect is using AWS Database Migration Service (AWS DMS) to perform the data migration. The migration is taking longer than expected, and the company wants to speed up the process. The company's network team has ruled out bandwidth as a limiting factor. Which actions should the solutions architect take to speed up the migration? (Select TWO.)

- A. Disable Multi-AZ on the target DB instance.
- B. Create a new DMS instance that has a larger instance size.
- C. Turn off logging on the target DB instance until the initial load is complete.
- D. Restart the DMS task on a new DMS instance with transfer acceleration enabled.
- E. Change the storage type on the target DB instance to Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2).

Answer: C, D

Explanation:

Question: 90

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

- A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.
- B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Answer: B

Explanation:

Question: 91

An ecommerce company is creating an application that requires a connection to a third-party payment service to process payments. The payment service needs to explicitly allow the public IP address of the server that is making the payment request. However, the company's security policies do not allow any server to be exposed directly to the public internet.

Which solution will meet these requirements?

- A. Provision an Elastic IP address. Host the application servers on Amazon EC2 instances in a private subnet. Assign the public IP address to the application servers.
- B. Create a NAT gateway in a public subnet. Host the application servers on Amazon EC2 instances in a private subnet. Route payment requests through the NAT gateway.
- C. Deploy an Application Load Balancer (ALB). Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the ALB.
- D. Set up an AWS Client VPN connection to the payment service. Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the VPN.

Answer: C

Explanation:

Question: 92

A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.

Which actions should the solutions architect take to protect the website from such an attack? (Select TWO.)

- A. Use AWS Shield Advanced to stop the DDoS attack.
- B. Configure Amazon GuardDuty to automatically block the attackers.
- C. Configure the website to use Amazon CloudFront for both static and dynamic content.
- D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
- D. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization

Answer: A, D

Explanation:

Question: 93

A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.

Which solution should a solutions architect recommend to meet these requirements?

- A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily

schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

Configure a backup window for the RDS DB Instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) B. to schedule snapshot deletions.

C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years

D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target Configure S3 Lifecycle policies to delete the snapshots after 2 years.

Answer: A

Explanation:

Question: 94

An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format The company is evaluating a disaster recovery solution to back up the dat

a. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.

Which solution meets these requirements MOST cost-effectively?

A. Amazon Elasticsearch Service (Amazon ES)

B. Amazon S3 Glacier

C. Amazon S3 Standard

D. Amazon RDS for PostgreSQL

Answer: A

Explanation:

Question: 95

A social media company is building a feature tor its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.

Which solution meets these requirements with the MOST scalability?

A. Upload files from the user's browser to the application servers Transfer the files to an Amazon S3 bucket.

B. Provision an AWS Storage Gateway file gateway. Upload files directly from the user's browser to the file gateway.

C. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user's browser into an S3 bucket

D. Provision an Amazon Elastic File System (Amazon EFS) file system. Upload files directly from the user's browser to the file system.

Answer: C

Explanation:

Question: 96

A company stores project information in a shared spreadsheet. The company wants to create a web application to replace the spreadsheet. The company has chosen Amazon DynamoDB to store the spreadsheet's data and is designing the web application to display the project information that is obtained from DynamoDB.

A solutions architect must design the web application's backend by using managed services that require minimal operational maintenance.

Which architectures meet these requirements? (Select TWO.)

- A. An Amazon API Gateway REST API accesses the project information that is in DynamoDB.
- B. An Elastic Load Balancer forwards requests to a target group with DynamoDB set up as the target.
- C. An Amazon API Gateway REST API invokes an AWS Lambda function. The Lambda function accesses DynamoDB.
- D. An Amazon Route 53 hosted zone routes requests to an AWS Lambda endpoint to invoke a Lambda function that accesses DynamoDB.
- E. An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that accesses DynamoDB.

Answer: A, E

Explanation:

Question: 97

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

- A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
- B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
- C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
- D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS Single Sign-On.

Answer: D

Explanation:

Question: 98

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2

Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

- A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.
- B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.
- C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.
- D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group.

Answer: D

Explanation:

Question: 99

The application's traffic is often low, but it occasionally grows significantly. During these sudden increases in traffic, DynamoDB returns throttling errors. The result is that error pages are displayed to end users.

What should a solutions architect do to reduce these errors?

- A. Change the DynamoDB table to use on-demand capacity mode.
- B. Create a DynamoDB read replica to scale the read traffic horizontally.
- C. Purchase DynamoDB reserved capacity of 1,000 RCUs and 500 WCUs.
- D. Configure the application to use strongly consistent reads for DynamoDB queries.

Answer: D

Explanation:

Question: 100

A solutions architect is designing the cloud architecture for a new application that is being deployed on AWS. The application's users will interactively download and upload files. Files that are more than 90 days old will be accessed less frequently than newer files, but all files need to be instantly available. The solutions architect must ensure that the application can scale to store petabytes of data with maximum durability.

Which solution meets these requirements?

- A. Store the files in Amazon S3 Standard. Create an S3 Lifecycle policy that moves objects that are more than 90 days old to S3 Glacier.
- B. Store the files in Amazon S3 Standard. Create an S3 Lifecycle policy that moves objects that are

- more than 90 days old to S3 Standard-Infrequent Access (S3 Standard-IA).
- C. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data that is more than 90 days old.
- D. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data that is more than 90 days old.

Answer: B

Explanation:

Question: 101

A company is launching a new application that will be hosted on Amazon EC2 instances. A solutions architect needs to design a solution that does not allow public IPv4 access that originates from the internet. However, the solution must allow the EC2 instances to make outbound IPv4 internet requests.

The initial design proposal shows that the EC2 instances would be located in two private subnets across two Availability Zones. The entire architecture must be highly available.

How should the solutions architect change the architecture to meet these requirements?

- A. Deploy a NAT gateway in public subnets in both Availability Zones. Create and configure one route table for each private subnet.
- B. Deploy an internet gateway in public subnets in both Availability Zones. Create and configure a shared route table for the private subnets.
- C. Deploy a NAT gateway in public subnets in both Availability Zones. Create and configure a shared route table for the private subnets.
- D. Deploy an egress-only internet gateway in public subnets in both Availability Zones. Create and configure one route table for each private subnet.

Answer: C

Explanation:

Question: 102

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynam
- B. Amazon DynamoDB global tables
- C. Amazon RDS for MySQL with Multi-AZ enabled
- D. Amazon RDS for MySQL with a cross-Region snapshot copy

Answer: A

Explanation:

Question: 103

A solutions architect is designing the architecture for a company website that is composed of static content. The company's target customers are located in the United States and Europe.

Which architecture should the solutions architect recommend to MINIMIZE cost?

Store the website files on Amazon S3 in the us-east-2 Region. Use an Amazon CloudFront distribution with the price class configured to limit the edge locations in use.

Store the website files on Amazon S3 in the us-east-2 Region. Use an Amazon CloudFront distribution with the price class configured to maximize the use of edge locations.

Store the website files on Amazon S3 in the us-east-2 Region and the eu-west-1 Region. Use an Amazon CloudFront geolocation routing policy to route requests to the closest Region to the user.

Store the website files on Amazon S3 in the us-east-2 Region and the eu-west-1 Region. Use an Amazon CloudFront distribution with an Amazon Route 53 latency routing policy to route requests to the closest Region to the user.

Answer: D

Explanation:

Question: 104

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.

How should a solution architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer create a new policy.
- B. Use service control policies to disable IAM across all account in the organizational unit.
- C. Prevent the developers from attaching any policies and duties to the security option team.
- D. Set an IAM permission boundary on the developer IAM role that explicitly denies of attaching the administrator policy

Answer: D

Explanation:

Question: 105

A healthcare computer stores highly sensitive records. Compliance requires that multiple copies be stored in different locations. Each record must be stored for 7 years. The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter.

What should a solutions architect recommend?

- A. Use Amazon S3 with cross-Region Region replication enabled. After 30 days. Transition the data to Amazon S3 Glacier using lifecycle policy.
- B. Use Amazon S3 with cross-origin resource sharing (CCRS) enabled. After 30 days. Transition on the data to Amazon S3 Glacier using a lifecycle policy.
- C. Use Amazon S3 with cross-origin replication enabled. After 30 days, transition the data to Amazon

S3 Glacier Deep Archive a lifecycle policy.

D. Use Amazon S3 with cross-origin resource sharing (CCRS) enabled. After 30 days, transition on the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.

Answer: C

Explanation:

Question: 106

A computer is reviewing a recent migration of a three-tier application to a VPC. The security team discover that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solution architect do to connect issue?

- A. Create security group rules using the instance ID as the source destination.
- B. Create security group rules using the security ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination
- D. Create security group rules using the subnet CIDR blocks as the source or destination

Answer: C

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

Question: 107

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials needs to be removed from the Lambda source code. The credentials must then be securely stored and rotated on a on-going basis to meet security policy requirements.

What should a solutions architect recommend meet these requirements?

- A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can review the password from CloudHSM given key ID.
- B. Store the password in AWS Secrets Manager . A associate the Lambda function with a role that can retrieve the password from secrets Manager given its secret ID.
- C. Move the database password to an environment variable associate the Lambda function Retrieve the password from the environment variable upon execution.
- D. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

Answer: B

Explanation:

Question: 108

A company receives data from millions of users totalling about 1 TB each day. The company provides its users with usage report going back 12 months. All usage data must be stored for at least 5 years to comply with regulatory and auditing requirements?
Which storage solution is MOST cost-effective?

- A. Store the data in Amazon S3 Standard. Set a lifecycle rule to transition the data to S3 Glacier Deep Archive after 1 year. Set a lifecycle rule to delete the data after 5 years.
- B. Store the data in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA). Set a lifecycle rule to transition the data to S3 Glacier after 1 year. Set the lifecycle rule to delete the data after 5 years.
- C. Store the data in Amazon S3 Standard. Set a lifecycle rule to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 year. Set a lifecycle rule to delete the data after 5 years.
- D. Store the data in Amazon S3 Standard. Set a lifecycle rule to transition the data to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Set a lifecycle rule to delete the data after 5 years.

Answer: A

Explanation:

Question: 109

A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have complained of timeouts. The architect uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests.

How should a solutions architect redesign the architecture to better respond to changing traffic?

- A. Configure a Network Load Balancer with a slow start configuration.
- B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.
- C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
- D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Answer: C

Explanation:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html#as-step-scaling-warmup>

"If you are creating a step policy, you can specify the number of seconds that it takes for a newly launched instance to warm up. Until its specified warm-up time has expired, an instance is not counted toward the aggregated metrics of the Auto Scaling group. Using the example in the Step Adjustments section, suppose that the metric gets to 60, and then it gets to 62 while the new instance is still warming up. The current capacity is still 10 instances, so 1 instance is added (10 percent of 10 instances). However, the desired capacity of the group is already 11 instances, so the scaling policy does not increase the desired capacity further. If the metric gets to 70 while the new instance is still warming up, we should add 3 instances (30 percent of 10 instances). However, the desired capacity of the group is already 11, so we add only 2 instances, for a new desired capacity of 13 instances"

Question: 110

A solution architect is designing a new service behind API Gateway. The request pattern for the service will be unpredictable and can change suddenly from 0 request to over 500 per second. The total size of the data that needs to be persisted database is currently less than 1 GB unpredictable future growth. Data can be queried using sampling key-value request.

Which combination of AWS services would meet these requirements? (Select TWO.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Answer: A, C

Explanation:

Question: 111

A company needs to store 160TB of data for an indefinite of time. The company must be able to use standard SQL and business intelligence tools to query all of the data.

a. The data will be queried no more than twice each month.

What is the MOST cost-effective solution that meets these requirements?

- A. Store the data in Amazon Aurora Serverless with MySQL. Use an SQL client to query the data.
- B. Store the data in Amazon S3. Use AWS Glue, Amazon Athena, JDBC and ODBC drivers to query the data.
- C. Store the data in an Amazon EMR cluster with EMR File System (EMRFS) as the storage layer use Apache Presto to query the data.
- D. Store a subset of the data in Amazon Redshift, and store the remaining data in Amazon S3. Use Amazon Redshift Spectrum to query the S3 data.

Answer: D

Explanation:

Question: 112

A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A possible architect needs design an optimal solution that requires minimal application changes.

Which method should the solution architect select?

- A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use DAX endpoint.
- B. Add DynamoDB read replicas to handle the increased read load the application to point to the read endpoint for the read replicas.
- C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
- D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to

point to the Redis cache endpoint of DynamoDB.

Answer: A

Explanation:

Topic 2, Exam Pool B

Question: 113

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical database from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElastiCache to cache the large database.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Answer: B

Explanation:

Question: 114

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.

How can these requirements be met?

- A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval capacity for the workload.
- B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway store data in Amazon retaining copies of frequently accessed data subnets locally.
- C. Deploy AWS Storage gateway using stored volume to store data locally Use Storage gateway asynchronously back up point-in-time snapshots of the data Amazon S3.
- D. Deploy AWS Direct Connects to connect with on-premises data center. Configure AWS Storage gateway to store data locally use storage gateway to asynchronously back up point-in-time snapshot of data Amazon S3.

Answer: B

Explanation:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html>

Question: 115

A company plans to store sensitive user data on Amazon S3 internal security compliance requirement mandate encryption of data before secured it to Amazon S3.

What should a solutions architect recommend to safely these requirements?

- A. Server-side encryption with customer-provided encryption keys.
- B. Client-side encryption with Amazon S3 managed encryption keys.
- C. Service-side encryption with keys stored in AWS Management Service (AWS KMS)
- D. Server-side encryption with a master stored in AWS Management Service (AWS KMS)

Answer: D

Explanation:

Question: 116

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.

Which storage solution should the solutions architect use?

- A. Amazon EBS
- B. Amazon EC2 instance store
- C. Amazon EFS
- D. Amazon S3

Answer: B

Explanation:

Question: 117

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

- A. Configure Amazon EFS storage and set the Active Directory domain for authentication
- B. Create an SMB Me share on an AWS Storage Gateway file gateway in two Availability Zones
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication

Answer: D

Explanation:

Question: 118

A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets. Each private subnet uses a NAT instance for Internet access. All images are stored in Amazon S3 buckets. The company is concerned about the data transfer costs between Amazon ECS and Amazon S3.

What should a solutions architect do to reduce costs?

- A. Configure a NAT gateway to replace the NAT instances
- B. Configure a gateway endpoint for traffic destined to Amazon S3
- C. Configure an interface endpoint for traffic destined to Amazon S3
- D. Configure Amazon CloudFront for the S3 bucket storing the images

Answer: C

Explanation:

Question: 119

A company runs a three-tier web application in a VPC across multiple Availability Zones. Amazon EC2 instances run in an Auto Scaling group for the application tier.

The company needs to make an automated scaling plan that will analyze each resource's daily and weekly historical workload trends. The configuration must scale resources appropriately according to both the forecast and live changes in utilization.

Which scaling strategy should a solutions architect recommend to meet these requirements?

- A. Implement dynamic scaling with step scaling based on average CPU utilization from the EC2 instances
- B. Enable predictive scaling to forecast and scale. Configure dynamic scaling with target tracking.
- C. Create an automated scheduled scaling action based on the traffic patterns of the web application.
- D. Set up a simple scaling policy. Increase the cool-down period based on the EC2 instance start-up time.

Answer: B

Explanation:

Question: 120

A company is using AWS to design a web application that will process insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type, must be responded to within 24 hours, and must not get lost. The solution must maximize operational efficiency and must minimize maintenance. Which solution meets these requirements?

- A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to use the Kinesis Client Library (KCL) to pull messages from its own data stream.
- B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic.

for each quote type Subscribe the Lambda function to its associated SNS topic Configure the application to publish requests tot quotes to the appropriate SNS topic

C. Create a single Amazon Simple Notification Service (Amazon SNS) topic Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type Configure each backend application server to use its own SQS queue

D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasucsearch Service (Amazon ES) cluster Configure the application to send messages to the proper delivery stream Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly

Answer: C

Explanation:

Question: 121

A solutions architect is designing the architecture for a software demonstration environment The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) The system will experience significant increases in traffic during working hours but is not required to operate on weekends.

Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Select TWO)

- A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate
- B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway
- C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions
- D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization
- E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends Revert to the default values at the start of the week

Answer: D, E

Explanation:

Question: 122

A company has recently updated its internal security standards The company must now ensure all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists The company is looking for a native, software-based AWS service to accomplish this goal

What should a solutions architect recommend as a solution?

- A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager
- B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in AWS KMS.
- C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material

and apply a routine to re-create a new key periodically and replace it in the CloudHSM cluster nodes

D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the Parameter Store

Answer: A

Explanation:

Question: 123

A company wants to host a web application on AWS that will communicate to a database within a VPC. The application should be highly available.

What should a solutions architect recommend?

- A. Create two Amazon EC2 instances to host the web servers behind a load balancer and then deploy the database on a large instance
- B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones
- C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet
- D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones

Answer: D

Explanation:

Question: 124

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing. 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.

Which set of services should a solutions architect recommend to meet these requirements?

- A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
- B. Amazon EBS for maximum performance, Amazon EFS for durable data storage and Amazon S3 Glacier for archival storage
- C. Amazon EC2 instance store for maximum performance. Amazon EFS for durable data storage and Amazon S3 for archival storage
- D. Amazon EC2 Instance store for maximum performance. Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Answer: A

Explanation:

Question: 125

A company that operates a web application on premises is preparing to launch a newer version of the application on AWS. The company needs to route requests to either the AWS-hosted or the on-premises-hosted application based on the URL query string. The on-premises application is not available from the Internet, and a VPN connection is established between Amazon VPC and the company's data center. The company wants to use an Application Load Balancer (ALB) for this launch. Which solution meets these requirements?"

- A. Use two ALBs: one for on premises and one for the AWS resource. Add hosts to each target group of each ALB. Route with Amazon Route 53 based on the URL query string.
- B. Use two ALBs; one for on premises and one for the AWS resource. Add hosts to the target group of each ALB. Create a software router on an EC2 instance based on the URL query string.
- C. Use one ALB with two target groups: one for the AWS resource and one for on premises. Add hosts to each target group of the ALB. Configure listener rules based on the URL query string.
- D. Use one ALB with two AWS Auto Scaling groups: one for the AWS resource and one for on premises. Add hosts to each Auto Scaling group. Route with Amazon Route 53 based on the URL query string.

Answer: C

Explanation:

Question: 126

A company is migrating its applications to AWS. Currently, applications that run on premises generate hundreds of terabytes of data that is stored on a shared file system. The company is running an analytics application in the cloud that runs hourly to generate insights from this data. The company needs a solution to handle the ongoing data transfer between the on-premises shared file system and Amazon S3. The solution also must be able to handle occasional interruptions in internet connectivity. Which solution should the company use for the data transfer to meet these requirements?"

- A. AWS DataSync
- B. AWS Migration Hub
- C. AWS Snowball Edge Storage Optimized
- D. AWS Transfer for SFTP

Answer: A

Explanation:

Question: 127

A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by 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 solution should a solutions architect recommend that has the LEAST amount of downtime?"

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

Answer: A

Explanation:

Question: 128

A company has a web application with sporadic usage patterns There is heavy usage at the beginning of each month moderate usage at the start of each week and unpredictable usage during the week The application consists of a web server and a MySQL database server running inside the data center The company would like to move the application to the AWS Cloud and needs to select a cost-effective database platform that will not require database modifications Which solution will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Answer: B

Explanation:

Question: 129

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings All application components will be deployed on the AWS infrastructure.

The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache

- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

Answer: A

Explanation:

Question: 130

A company is migrating a NoSQL database cluster to Amazon EC2. The database automatically replicates data to maintain at least three copies of the data I/O throughput of the servers is the highest priority.

Which instance type should a solutions architect recommend for the migration?

- A. Storage optimized instances with instance store
- B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume
- C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled
- D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

Answer: A

Explanation:

Question: 131

A company has a website running on Amazon EC2 Instances across two Availability Zones The company is expecting spikes in traffic on specific holidays and wants to provide a consistent user experience.

How can a solutions architect meet this requirement?

- A. Use step scaling
- B. Use simple scaling
- C. Use lifecycle hooks
- D. Use scheduled scaling

Answer: D

Explanation:

Question: 132

A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer Amazon Route 53 is used for the DNS The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down. How should the company deploy this solution?

- A. Use Amazon S3 website hosting for the backup website and a Route 53 failover routing policy
- B. Use Amazon S3 website hosting for the backup website and a Route 53 latency routing policy
- C. Deploy the application in another AWS Region and use ELB health checks for failover routing.

D. Deploy the application in another AWS Region and use server-side redirection on the primary website

Answer: A

Explanation:

<https://aws.amazon.com/blogs/aws/create-a-backup-website-using-route-53-dns-failover-and-s3-website-hosting/>

Question: 133

A company is hosting 60 TB of production-level data in an Amazon S3 bucket. A solutions architect needs to bring that data on premises for quarterly audit requirements. This export of data must be encrypted while in transit. The company has low network bandwidth in place between AWS and its on-premises data center.

What should the solutions architect do to meet these requirements?

- A. Deploy AWS Migration Hub with 90-day replication windows for data transfer
- B. Deploy an AWS Storage Gateway volume gateway on AWS. Enable a 90-day replication window to transfer the data.
- C. Deploy Amazon Elastic File System (Amazon EFS), with lifecycle policies enabled, on AWS. Use it to transfer the data.
- D. Deploy an AWS Snowball device in the on-premises data center after completing an export job request in the AWS Snowball console.

Answer: D

Explanation:

Question: 134

An e-commerce company has noticed performance degradation of its Amazon RDS-based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.

What should the solutions architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Answer: C

Explanation:

Question: 135

A user wants to list the IAM role that is attached to their Amazon EC2 Instance. The user has login access to the EC2 instance but does not have IAM permissions. What should a solutions architect do to retrieve this information?

A)

Run the following EC2 command:

```
curl http://169.254.169.254/latest/meta-data/iam/info
```

B)

Run the following EC2 command:

```
curl http://169.254.169.254/latest/user-data/iam/info
```

C)

Run the following EC2 command:

```
http://169.254.169.254/latest/dynamic/instance-identity/
```

D)

Run the following AWS CLI command:

```
aws iam get-instance-profile --instance-profile-name ExampleInstanceProfile
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Question: 136

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff. What should the solutions architect recommend?

A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.

B. Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory on the current EC2 instance.

C. Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active Directory domain controller running on the current EC2 instance.

D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: A

Explanation:

Question: 137

A company has established a new AWS account. The account is newly provisioned and no changes have been made to the default settings. The company is concerned about the security of the AWS account root user.

What should be done to secure the root user?

- A. Create IAM users for daily administrative tasks. Disable the root user.
- B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
- C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
- D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

Answer: B

Explanation:

Question: 138

A company uses on-premises servers to host its application. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications. Which combination of actions should a solutions architect take to meet these requirements? (Select TWO.)

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway File gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway Volume gateway to replace the block storage.
- E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

Answer: B, D

Explanation:

Question: 139

A security team needs to enforce the rotation of all IAM users' access keys every 90 days. If an access key is found to be older, the key must be made inactive and removed. A solutions architect must create a solution that will check for and remediate any keys older than 90 days. Which solution meets these requirements with the LEAST operational effort?

- A. Create an AWS Config rule to check for the key age. Configure the AWS Config rule to run an AWS Batch job to remove the key.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Configure the rule to run an AWS Batch job to remove the key.

- C. Create an AWS Config rule to check for the key age Define an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule an AWS Lambda function to remove the key
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age Define an EventBridge (CloudWatch Events) rule to run an AWS Batch job to remove the key

Answer: C

Explanation:

Question: 140

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries. Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries

Answer: C

Explanation:

Question: 141

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture. What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed
- B. Use Amazon CloudWatch Logs to store the logs. Run SQL queries as needed from the Amazon CloudWatch console
- C. Use Amazon Athena directly with Amazon S3 to run the queries as needed
- D. Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed

Answer: B

Explanation:

Question: 142

A company has multiple AWS accounts for various departments. One of the departments wants to

share an Amazon S3 bucket with all other departments. Which solution will require the LEAST amount of effort?

- A. Enable cross-account S3 replication for the bucket
- B. Create a pre-signed URL for the bucket and share it with other departments
- C. Set the S3 bucket policy to allow cross-account access to other departments
- D. Create IAM users for each of the departments and configure a read-only IAM policy

Answer: C

Explanation:

Question: 143

A company wants to build an immutable infrastructure for its software applications. The company wants to test the software applications before sending traffic to them. The company seeks an efficient solution that limits the effects of application bugs.

Which combination of steps should a solutions architect recommend? (Select TWO)

- A. Use AWS CloudFormation to update the production infrastructure and roll back the stack if the update fails
- B. Apply Amazon Route 53 weighted routing to test the staging environment and gradually increase the traffic as the tests pass
- C. Apply Amazon Route 53 failover routing to test the staging environment and fail over to the production environment if the tests pass
- D. Use AWS CloudFormation with a parameter set to the staging value in a separate environment other than the production environment
- E. Use AWS CloudFormation to deploy the staging environment with a snapshot deletion policy and reuse the resources in the production environment if the tests pass

Answer: A, E

Explanation:

Question: 144

A company hosts its static website content from an Amazon S3 bucket in the us-east-1 Region. Content is made available through an Amazon CloudFront origin pointing to that bucket. Cross-Region replication is set up to create a second copy of the bucket in the ap-southeast-1 Region. Management wants a solution that provides greater availability for the website.

Which combination of actions should a solutions architect take to increase availability? (Select TWO.)

- A. Add both buckets to the CloudFront origin
- B. Configure failover routing in Amazon Route 53
- C. Create a record in Amazon Route 53 pointing to the replica bucket
- D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket
- E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary

Answer: B, E

Explanation:

Question: 145

A solutions architect is designing a multi-Region disaster recovery solution (or an application that will provide public API access). The application will use Amazon EC2 instances with a userdata script to load application code and an Amazon RDS for MySQL database. The Recovery Time Objective (RTO) is 3 hours and the Recovery Point Objective (RPO) is 24 hours.

Which architecture would meet these requirements at the LOWEST cost/?

- A. Use an Application Load Balancer for Region failover. Deploy new EC2 instances with the userdata script. Deploy separate RDS instances in each Region.
- B. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script. Create a read replica of the RDS instance in a backup Region.
- C. Use Amazon API Gateway for the public APIs and Region failover. Deploy new EC2 instances with the userdata script. Create a MySQL read replica of the RDS instance in a backup Region.
- D. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script for APIs, and create a snapshot of the RDS instance daily for a backup. Replicate the snapshot to a backup Region.

Answer: C

Explanation:

Question: 146

Application developers have noticed that a production application is very slow when business reporting users run large production reports against the Amazon RDS instance backing the application. The CPU and memory utilization metrics for the RDS instance do not exceed 60% while the reporting queries are running. The business reporting users must be able to generate reports without affecting the application's performance.

Which action will accomplish this?

- A. Increase the size of the RDS instance.
- B. Create a read replica and connect the application to it.
- C. Enable multiple Availability Zones on the RDS instance.
- D. Create a read replica and connect the business reports to it.

Answer: D

Explanation:

Question: 147

A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple

Amazon EC2 instances

What should the solutions architect do to reduce the overall data transfer costs?

- A. Place all the EC2 instances in an Auto Scaling group
- B. Place all the EC2 instances in the same AWS Region
- C. Place all the EC2 instances in the same Availability Zone
- D. Place all the EC2 instances in private subnets in multiple Availability Zones

Answer: C

Explanation:

Question: 148

A company maintains about 300 TB in Amazon S3 Standard storage month after month. The S3 objects are each typically around 50 GB in size and are frequently replaced with multipart uploads by their global application. The number and size of S3 objects remain constant but the company's S3 storage costs are increasing each month.

How should a solutions architect reduce costs in this situation?

- A. Switch from multipart uploads to Amazon S3 Transfer Acceleration
- B. Enable an S3 Lifecycle policy that deletes incomplete multipart uploads
- C. Configure S3 inventory to prevent objects from being archived too quickly
- D. Configure Amazon CloudFront to reduce the number of objects stored in Amazon S3

Answer: B

Explanation:

Question: 149

A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers. In an Auto Scaling group, spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage

Answer: B

Explanation:

Question: 150

A solutions architect plans to convert a company's monolithic web application into a multi-tier application. The company wants to avoid managing its own infrastructure. The minimum requirements for the web application are high availability, scalability, and regional low latency during peak hours. The solution should also store and retrieve data with millisecond latency using the application's API.

Which solution meets these requirements?

- A. Use AWS Fargate to host the web application with backend Amazon RDS Multi-AZ DB instances.
- B. Use Amazon API Gateway with an edge-optimized API endpoint, AWS Lambda for compute, and Amazon DynamoDB as the data store.
- C. Use an Amazon Route 53 routing policy with geolocation that points to an Amazon S3 bucket with static website hosting and Amazon DynamoDB as the data store.
- D. Use an Amazon CloudFront distribution that points to an Elastic Load Balancer with an Amazon EC2 Auto Scaling group, along with Amazon RDS Multi-AZ DB instances.

Answer: B

Explanation:

Question: 151

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.

How can a solutions architect ensure that the application has permission to access Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS and then relaunch the container.
- B. Create an IAM role with S3 permissions and then specify that role as the taskRoleArn in the task definition.
- C. Create a security group that allows access from Amazon ECS to Amazon S3 and update the launch configuration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Answer: B

Explanation:

Question: 152

A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling. Management is concerned that the company is over-provisioning its infrastructure, especially at the front end of the three-tier application. A solutions architect needs to ensure costs are optimized without impacting performance.

What should the solutions architect do to accomplish this?

- A. Use Auto Scaling with Reserved Instances.

- B. Use Auto Scaling with a scheduled scaling policy
- C. Use Auto Scaling with the suspend-resume feature.
- D. Use Auto Scaling with a target tracking scaling policy

Answer: D

Explanation:

Question: 153

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.

Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone
- B. Launch the EC2 instances in a spread placement group in one Availability Zone
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

Answer: A

Explanation:

Question: 154

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Answer: B

Explanation:

Question: 155

A company wants to build an online marketplace application on AWS as a set of loosely coupled

microservices For this application, when a customer submits a new order two microservices should handle the event simultaneously The Email microservice will send a confirmation email and the OrderProcessing microservice will start the order delivery process If a customer cancels an order, the OrderCancellation and Email microservices should handle the event simultaneously.

A solutions architect wants to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) to design the messaging between the microservices.

How should the solutions architect design the solution?

- A. Create a single SQS queue and publish order events to it The Email, OrderProcessing and OrderCancellation microservices can then consume messages off the queue
- B. Create three SNS topics for each microservice Publish order events to the three topics Subscribe each of the Email OrderProcessing, and OrderCancellation microservices to its own topic
- C. Create an SNS topic and publish order events to it Create three SQS queues for the Email OrderProcessing and OrderCancellation microservices Subscribe all SQS queues to the SNS topic with message filtering
- D. Create two SQS queues and publish order events to both queues simultaneously One queue is for the Email and OrderProcessing microservices The second queue is for the Email and Order Cancellation microservices

Answer: C

Explanation:

Question: 156

A solutions architect must migrate a Windows Internet Information Services (IIS) web application to AWS The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS) The solutions architect has proposed migrating the MS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances

Which replacement to the on-premises file share is MOST resilient and durable?

- A. Migrate the file share to Amazon RDS
- B. Migrate the file share to AWS Storage Gateway
- C. Migrate the file share to Amazon FSx for Windows File Server
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS)

Answer: C

Explanation:

Question: 157

A company wants to provide users with access to AWS resources. The company has 1,500 users and manages their access to on-premises resources through Active Directory user groups on the corporate network However, the company does not want users to have to maintain another identity to access the resources A solutions architect must manage user access to the AWS resources while preserving access to the on-premises resources

What should the solutions architect do to meet these requirements?

- A. Create an IAM user for each user in the company Attach the appropriate policies to each user
- B. Use Amazon Cognito with an Active Directory user pool Create roles with the appropriate policies attached
- C. Define cross-account roles with the appropriate policies attached Map the roles to the Active Directory groups
- D. Configure Security Assertion Markup Language (SAML) 2.0-based federation Create roles with the appropriate policies attached Map the roles to the Active Directory groups

Answer: D

Explanation:

Question: 158

A weather forecasting company needs to process hundreds of gigabytes of data with sub-millisecond (second) latency. The company has a high performance computing (HPC) environment in its data center and wants to expand its forecasting capabilities

A solutions architect must identify a highly available cloud storage solution that can handle large amounts of sustained throughput. Files that are stored in the solution should be accessible to thousands of compute instances that will simultaneously access and process the entire dataset

What should the solutions architect do to meet these requirements?

- A. Use Amazon FSx for Lustre scratch file systems.
- B. Use Amazon FSx for Lustre persistent file systems
- C. Use Amazon Elastic File System (Amazon EFS) with Bursting Throughput mode
- D. Use Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode

Answer: C

Explanation:

Question: 159

A company has deployed a business-critical application in the AWS Cloud. The application uses Amazon EC2 instances that run in the us-east-1 Region. The application uses Amazon S3 for storage of all critical data.

To meet compliance requirements, the company must create a disaster recovery (DR) plan that provides the capability of a full failover to another AWS Region.

What should a solutions architect recommend for this DR plan?

- A. Deploy the application to multiple Availability Zones in us-east-1. Create a resource group in AWS Resource Groups. Turn on automatic failover for the application to use a predefined recovery Region.
- B. Perform a virtual machine (VM) export by using AWS Import/Export on the existing EC2 instances. Copy the exported instances to the destination Region. In the event of a disaster, provision new EC2 instances from the exported EC2 instances.
- C. Create snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the EC2 instances in us-east-1. Copy the snapshots to the destination Region. In the event of a disaster,

provision new EC2 instances from the EBS snapshots

D. Use S3 Cross-Region Replication for the data that is stored in Amazon S3 Create an AWS CloudFormation template for the application with an S3 bucket parameter In the event of a disaster deploy the template to the destination Region and specify the local S3 bucket as the parameter

Answer: D

Explanation:

Question: 160

A company has thousands of edge devices that collectively generate 1 TB of status alerts each day Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis

The company wants a highly available solution However the company needs to minimize costs and does not want to manage additional infrastructure Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days

What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days

B Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days

C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon Elasticsearch Service (Amazon ES) cluster Set up the Amazon ES cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days

D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts and set the message retention period to 14 days Configure consumers to poll the SQS queue check the age of the message and analyze the message data as needed If the message is 14 days old the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue

Answer: A

Explanation:

Question: 161

A solutions architect is optimizing a website for an upcoming musical event Videos of the performances will be streamed in real time and then will be available on demand The event is expected to attract a global online audience

Which service will improve the performance of both the real-time and on-demand streaming?

A. Amazon CloudFront

B. AWS Global Accelerator

- C. Amazon Route 53
- D. Amazon S3 Transfer Acceleration

Answer: A

Explanation:

Question: 162

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements'?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling EC2_INSTANCE_LAUNCH events.

Answer: B

Explanation:

Question: 163

A company runs an AWS Lambda function in private subnets in a VPC. The subnets have a default route to the internet through an Amazon EC2 NAT instance. The Lambda function processes input data and saves its output as an object to Amazon S3.

Intermittently, the Lambda function times out while trying to upload the object because of saturated traffic on the NAT instance's network. The company wants to access Amazon S3 without traversing the internet.

Which solution will meet these requirements'?

- A. Replace the EC2 NAT instance with an AWS managed NAT gateway.
- B. Increase the size of the EC2 NAT instance in the VPC to a network optimized instance type.
- C. Provision a gateway endpoint for Amazon S3 in the VPC. Update the route tables of the subnets accordingly.
- D. Provision a transit gateway. Place transit gateway attachments in the private subnets where the Lambda function is running.

Answer: C

Explanation:

Question: 164

A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only. What should a solutions architect do to protect against data loss? (Select TWO.)

- A. Enable versioning on the S3 bucket
- B. Enable access logging on the S3 bucket.
- C. Enable server-side encryption on the S3 bucket.
- D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.
- E. Use MFA Delete to require multi-factor authentication to delete an object.

Answer: A, E

Explanation:

Question: 165

A company hosts a training site on a fleet of Amazon EC2 instances. The company anticipates that its new course which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week

What should a solutions architect do to minimize the anticipated server load?

- A. Store the videos in Amazon ElastiCache for Redis Update the web servers to serve the videos using the ElastiCache API
- B. Store the videos in Amazon Elastic File System (Amazon EFS) Create a user data script for the web servers to mount the EPS volume
- C. Store the videos in an Amazon S3 bucket Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket Restrict Amazon S3 access to the OAI
- D. Store the videos in an Amazon S3 bucket Create an AWS Storage Gateway file gateway to access the S3 bucket Create a user data script for the web servers to mount the file gateway.

Answer: C

Explanation:

Question: 166

A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud The company needs the ability to use SMB clients to access data solution must be fully managed.

Which AWS solution meets these requirements?

- A. Create an AWS DataSync task that shares the data as a mountable file system Mount the file system to the application server
- B. Create an Amazon EC2 Windows instance Install and configure a Windows file share role on the instance Connect the application server to the file share
- C. Create an Amazon FSx for Windows File Server file system Attach the file system to the origin server Connect the application server to the file system

D. Create an Amazon S3 bucket Assign an IAM role to the application to grant access to the S3 bucket
Mount the S3 bucket to the application server

Answer: C

Explanation:

Question: 167

An application uses an Amazon RDS MySQL DB instance The RDS database is becoming low on disk space A solutions architect wants to increase the disk space without downtime Which solution meets these requirements with the LEAST amount of effort?

- A. Enable storage autoscaling in RDS
- B. Increase the RDS database instance size
- C. Change the RDS database instance storage type to Provisioned IOPS
- D. Back up the RDS database increase the storage capacity restore the database and stop the previous instance

Answer: A

Explanation:

Question: 168

A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users Dunning startup, the models need to load up to 10 GB of data from Amazon S3 into memory, out they do not need disk access Most of the models are used sporadically but the users expect all of them to be highly available and accessible with low latency. Which solution meets the requirements and is MOST cost-effective?

- A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model
- B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model
- C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model
- D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model

Answer: D

Explanation:

Question: 169

A company has hired an external vendor to perform work in the company's AWS account The vendor uses an automated tool that is hosted in an AWS account that the vendor owns The vendor does not have IAM access to the company's AWS account
How should a solutions architect grant this access to the vendor?

- A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
- B. Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user (or the permissions that the vendor requires).
- C. Create an IAM group in the company's account. Add the tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.
- D. Create a new identity provider by choosing "AWS account" as the provider type in the IAM console. Supply the vendor's AWS account ID and user name. Attach the appropriate IAM policies to the new provider for the permissions that the vendor requires.

Answer: B

Explanation:

Question: 170

A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection to the bastion host and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO)

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

Answer: B, E

Explanation:

Question: 171

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords. What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account.
- B. Set a password policy for each IAM user in the AWS account.

- C. Use third-party vendor software to set password requirements
- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements

Answer: A

Explanation:

Question: 172

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

- A. Purchase Reserved instances that specify the Region needed
- B. Create an On Demand Capacity Reservation that specifies the Region needed
- C. Purchase Reserved instances that specify the Region and three Availability Zones needed
- D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed

Answer: D

Explanation:

Question: 173

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution. Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files
- B. Use cross-Region replication to all Regions
- C. Use the geoproximity feature of Amazon Route 53
- D. Use Amazon CloudFront with the S3 bucket as its origin

Answer: D

Explanation:

Question: 174

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet. What should the solutions architect do to accomplish this? (Select TWO.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB
- C. Create a new DynamoDB table that uses the endpoint

- D. Create an ENI for the endpoint in each of the subnets of the VPC
- E. Create a security group entry in the default security group to provide access

Answer: A, B

Explanation:

Question: 175

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However, the company's security policy states that any external service cannot initiate a connection to the EC2 instances.

What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table
- B. Create an internet gateway and make it the destination of the subnet's route table
- C. Create a virtual private gateway and make it the destination of the subnet's route table
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table

Answer: D

Explanation:

Question: 176

A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation. The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses.

What should a solutions architect recommend to support this workload?

- A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.
- B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
- C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.
- D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

Answer: C

Explanation:

Question: 177

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached. Which solution provides the LOWEST data transfer egress cost for the company?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet
- B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region

Answer: D

Explanation:

Question: 178

A company is deploying an application that processes streaming data in near-real time. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to provide the lowest possible latency between nodes. Which networking solution meets these requirements?

- A. Place the EC2 instances in multiple VPCs and configure VPC peering
- B. Attach an Elastic Fabric Adapter (EFA) to each EC2 instance
- C. Run the EC2 instances in a spread placement group
- D. Use Amazon Elastic Block Store (Amazon EBS) optimized instance types

Answer: C

Explanation:

Question: 179

A company has an application that ingests incoming messages. Dozens of other applications and microservices then quickly consume these messages. The number of messages varies drastically and sometimes increases suddenly to 100,000 each second. The company wants to decouple the solution and increase scalability. Which solution meets these requirements?

- A. Persist the messages to Amazon Kinesis Data Analytics. Configure the consumer applications to read and process the messages.
- B. Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group to scale the number of EC2 instances based on CPU metrics.
- C. Write the messages to Amazon Kinesis Data Streams with a single shard. Use an AWS Lambda

function to preprocess messages and store them in Amazon DynamoDB Configure the consumer applications to read from DynamoDB to process the messages

D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions Configure the consumer applications to process the messages from the queues

Answer: D

Explanation:

Question: 180

A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53 The company occasionally experiences a timeout error when attempting to browse the application The networking team finds that some DNS queries return IP addresses of unhealthy instances resulting in the timeout error

What should a solutions architect implement to overcome these timeout errors?

- A. Create a Route 53 simple routing policy record for each EC2 instance Associate a health check with each record
- B. Create a Route 53 failover routing policy record for each EC2 instance Associate a health check with each record
- C. Create an Amazon CloudFront distribution with EC2 instances as its origin Associate a health check with the EC2 instances
- D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances Route to the ALB from Route53

Answer: D

Explanation:

Question: 181

A company is running an online transaction processing (OLTP) workload on AWS This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment Daily database snapshots are taken from this instance

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it Enable encryption on the DB instance
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS) Restore encrypted snapshot to an existing DB instance
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS)

Answer: C

Explanation:

Question: 182

A company runs a web-based portal that provides users with global breaking news local alerts, and weather updates The portal delivers each user a personalized view by using a mixture of static and dynamic content Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB) The company wants the portal to provide this content to its users across the world as quickly as possible

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

- A. Deploy the application stack in a single AWS Region Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin
- B. Deploy the application stack in two AWS Regions Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region
- C. Deploy the application stack in a single AWS Region Use Amazon CloudFront to serve the static content Serve the dynamic content directly from the ALB
- D. Deploy the application stack in two AWS Regions Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region

Answer: A

Explanation:

Question: 183

A company has an automobile sales website that stores its listings in a database on Amazon RDS When an automobile is sold the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

- A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume
- B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume
- C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics Use AWS Lambda functions to update the targets
- D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues Use AWS Lambda functions to update the targets

Answer: D

Explanation:

Question: 184

A solutions architect needs to design a highly available application consisting of web, application and database tiers. HTTPS content delivery should be as close to the edge as possible with the least delivery time.

Which solution meets these requirements and is MOST secure?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Answer: B

Explanation:

Question: 185

A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zones.

What should a solutions architect do to meet this requirement?

- A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.
- B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.
- C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.
- D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Answer: C

Explanation:

Question: 186

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

- A. Use a VPC endpoint for DynamoDB
- B. Use a NAT gateway in a public subnet
- C. Use a NAT instance in a private subnet
- D. Use the internet gateway attached to the VPC

Answer: A

Explanation:

Question: 187

A company recently launched its website to serve content to its global user base. The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin. How should a solutions architect optimize high availability for the application?

- A. Use `lambda@Edge` for CloudFront
- B. Use Amazon S3 Transfer Acceleration for CloudFront
- C. Configure another EC2 instance in a different Availability Zone as part of the origin group
- D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone

Answer: A

Explanation:

Question: 188

A company runs an application on a large fleet of Amazon EC2 instances. The application reads and writes entries into an Amazon DynamoDB table. The size of the DynamoDB table continuously grows, but the application needs only data from the last 30 days. The company needs a solution that minimizes cost and development effort. Which solution meets these requirements?

- A. Use an AWS CloudFormation template to deploy the complete solution. Redeploy the CloudFormation stack every 30 days, and delete the original stack.
- B. Use an EC2 instance that runs a monitoring application from AWS Marketplace. Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table. Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.
- C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. Configure the Lambda function to delete items in the table that are older than 30 days.
- D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.

Answer: D

Explanation:

Question: 189

A solution architect has created a new AWS account and must secure AWS account root user access. Which combination of actions will accomplish this? (Select TWO)

- A. Ensure the root user uses a strong password
- B. Enable multi-factor authentication to the root user
- C. Store root user access keys in an encrypted Amazon S3 bucket
- D. Add the root user to a group containing administrative permissions
- E. Apply the required permissions to the root user with an inline policy document

Answer: A, B

Explanation:

Question: 190

A company receives structured and semi-structured data from various sources once every day. A solutions architect needs to design a solution that leverages big data processing frameworks. The data should be accessible using SQL queries and business intelligence tools. What should the solutions architect recommend to build the MOST high-performing solution?

- A. Use AWS Glue to process data and Amazon S3 to store data
- B. Use Amazon EMR to process data and Amazon Redshift to store data
- C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data
- D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data

Answer: A

Explanation:

Question: 191

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks. Which additional configuration strategy should the solutions architect use to meet these requirements?

- A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
- C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.

D. Create a network ACL for the web servers and allow port 443 from the load balancer Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group

Answer: C

Explanation:

Question: 192

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard A solutions architect needs to design a solution that can handle large traffic spikes process the mobile game updates in order of receipt and store the processed updates in a highly available database The company also wants to minimize the management overhead required to maintain the solution

What should the solutions architect do to meet these requirements?

- A. Push score updates to Amazon Kinesis Data Streams Process the updates in Kinesis Data Streams with AWS Lambda Store the processed updates in Amazon DynamoDB
- B. Push score updates to Amazon Kinesis Data Streams Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling Store the processed updates in Amazon Redshift
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic Subscribe an AWS Lambda function to the SNS topic to process the updates Store the processed updates in a SQL database running on Amazon EC2
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue Store the processed updates in an Amazon RDS Multi-AZ DB instance

Answer: A

Explanation:

<https://docs.aws.amazon.com/streams/latest/dev/introduction.html>

You can use Amazon Kinesis Data Streams to collect and process large streams of data records in real time. You can use Kinesis Data Streams for rapid and continuous data intake and aggregation. The type of data used can include IT infrastructure log data, application logs, social media, market data feeds, and web clickstream data. Because the response time for the data intake and processing is in real time, the processing is typically lightweight.

Question: 193

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard A solutions architect needs to design a solution that can handle large traffic spikes process the mobile game updates in order of receipt and store the processed updates in a highly available database The company also wants to minimize the management overhead required to maintain the solution

What should the solutions architect do to meet these requirements?

- A. Push score updates to Amazon Kinesis Data Streams Process the updates in Kinesis Data Streams with AWS Lambda Store the processed updates in Amazon DynamoDB

- B. Push score updates to Amazon Kinesis Data Streams Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling Store the processed updates in Amazon Redshift
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic Subscribe an AWS Lambda function to the SNS topic to process the updates Store the processed updates in a SQL database running on Amazon EC2
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue Store the processed updates in an Amazon RDS Multi-AZ DB instance

Answer: A

Explanation:

Question: 194

A company is building a new furniture inventory application The company has deployed the application on a fleet of Amazon EC2 instances across multiple Availability Zones The EC2 instances run behind an Application Load Balancer (ALB) in their VPC

A solutions architect has observed that incoming traffic seems to favor one EC2 instance resulting in latency for some requests

What should the solutions architect do to resolve this issue?

- A. Disable session affinity (sticky sessions) on the ALB
- B. Replace the ALB with a Network Load Balancer
- C. Increase the number of EC2 instances in each Availability Zone
- D. Adjust the frequency of the health checks on the ALB's target group

Answer: B

Explanation:

Question: 195

A startup company is using the AWS Cloud to develop a traffic control monitoring system for a large city The system must be highly available and must provide near-real-time results for residents and city officials even during peak events

Gigabytes of data will come in daily from IoT devices that run at intersections and freeway ramps across the city The system must process the data sequentially to provide the correct timeline However results need to show only what has happened in the last 24 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy Amazon Kinesis Data Firehose to accept incoming data from the IoT devices and write the data to Amazon S3 Build a web dashboard to display the data from the last 24 hours
- B. Deploy an Amazon API Gateway API endpoint and an AWS Lambda function to process incoming data from the IoT devices and store the data in Amazon DynamoDB Build a web dashboard to display the data from the last 24 hours
- C. Deploy an Amazon API Gateway API endpoint and an Amazon Simple Notification Service (Amazon SNS) topic to process incoming data from the IoT devices Write the data to Amazon Redshift Build a web dashboard to display the data from the last 24 hours

D. Deploy an Amazon Simple Queue Service (Amazon SQS) FIFO queue and an AWS Lambda function to process incoming data from the IoT devices and store the data in an Amazon RDS DB instance Build a web dashboard to display the data from the last 24 hours

Answer: D

Explanation:

Question: 196

A recently created startup built a three-tier web application. The front end has static content The application layer is based on microservices User data is stored as JSON documents that need to be accessed with low latency. The company expects regular traffic to be low during the first year with peaks in traffic when it publicizes new features every month. The startup team needs to minimize operational overhead costs

What should a solutions architect recommend to accomplish this?

- A. Use Amazon S3 static website hosting to store and serve the front end Use AWS Elastic Beanstalk for the application layer Use Amazon DynamoDB to store user data
- B. Use Amazon S3 static website hosting to store and serve the front end Use Amazon Elastic Kubernetes Service (Amazon EKS) for the application layer Use Amazon DynamoDB to store user data
- C. Use Amazon S3 static website hosting to store and serve the front end Use Amazon API Gateway and AWS Lambda function for the application layer Use Amazon DynamoDB to store user data
- D. Use Amazon S3 static website hosting to store and serve the front end Use Amazon API Gateway and AWS Lambda function for the application layer Use Amazon RDS with read replicas to store user data

Answer: C

Explanation:

Question: 197

A company is building a web application that serves a content management system The content management system runs on Amazon EC2 instances behind an Application Load Balancer (ALB) The EC2 instances run in an Auto Scaling group across multiple Availability Zones Users are constantly adding and updating files blogs and other website assets in the content management system

A solutions architect must implement a solution in which all the EC2 instances share up-to-date website content with the least possible lag time

Which solution meets these requirements?

- A. Update the EC2 user data in the Auto Scaling group lifecycle policy to copy the website assets from the EC2 instance that was launched most recently Configure the ALB to make changes to the website assets only on the newest EC2 instance
- B. Copy the website assets to an Amazon Elastic File System (Amazon EFS) file system Configure each EC2 instance to mount the EFS file system locally Configure the website hosting application to reference the website assets that are stored in the EFS file system
- C. Copy the website assets to an Amazon S3 bucket Ensure that each EC2 instance downloads the website assets from the S3 bucket to the attached Amazon Elastic Block Store (Amazon EBS) volume

Run the S3 sync command once each hour to keep files up to date

D. Restore an Amazon Elastic Block Store (Amazon EBS) snapshot with the website assets Attach the EBS snapshot as a secondary EBS volume when a new EC2 instance is launched Configure the website hosting application to reference the website assets that are stored in the secondary EBS volume

Answer: B

Explanation:

Question: 198

A company has a three-tier environment on AWS that ingests sensor data from its users' devices The traffic flows through a Network Load Balancer (NLB) then to Amazon EC2 instances for the web tier and finally to EC2 instances for the application tier that makes database calls What should a solutions architect do to improve the security of data in transit to the web tier?

- A. Configure a TLS listener and add the server certificate on the NLB
- B. Configure AWS Shield Advanced and enable AWS WAF on the NLB
- C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS)

Answer: A

Explanation:

Question: 199

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an m-memory database storage solution that performs faster and provides high availability using data replication. Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

Explanation:

Question: 200

A company has designed an application where users provide small sets of textual data by calling a public API The application runs on AWS and includes a public Amazon API Gateway API that forwards requests to an AWS Lambda function for processing The Lambda function then writes the data to an Amazon Aurora Serverless database for consumption

The company is concerned that it could lose some user data if a Lambda function fails to process the

request property or reaches a concurrency limit.

What should a solutions architect recommend to resolve this concern?

- A. Split the existing Lambda function into two Lambda functions Configure one function to receive API Gateway requests and put relevant items into Amazon Simple Queue Service (Amazon SQS) Configure the other function to read items from Amazon SQS and save the data into Aurora
- B. Configure the Lambda function to receive API Gateway requests and write relevant items to Amazon ElastiCache Configure ElastiCache to save the data into Aurora
- C. Increase the memory for the Lambda function Configure Aurora to use the Multi-AZ feature
- D. Split the existing Lambda function into two Lambda functions Configure one function to receive API Gateway requests and put relevant items into Amazon Simple Notification Service (Amazon SNS) Configure the other function to read items from Amazon SNS and save the data into Aurora

Answer: A

Explanation:

Question: 201

A company has data stored in an on-premises data center that is used by several on-premises applications The company wants to maintain its existing application environment and be able to use AWS services for data analytics and future visualizations

Which storage service should a solutions architect recommend?

- A. Amazon Redshift
- B. AWS Storage Gateway for files
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Elastic File System (Amazon EFS)

Answer: B

Explanation:

Question: 202

A developer has a script to generate daily reports that users previously ran manually The script consistently completes in under 10 minutes The developer needs to automate this process in a cost-effective manner.

Which combination of services should the developer use? (Select TWO.)

- A. AWS Lambda
- B. AWS CloudTrail
- C. Cron on an Amazon EC2 instance
- D. Amazon EC2 On-Demand Instance with user data
- E. Amazon EventBridge {Amazon CloudWatch Events}

Answer: A,E

Explanation:

Question: 203

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases. What should a solutions architect recommend?

- A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns
- B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm
- C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm
- D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm

Answer: C

Explanation:

Question: 204

A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows. What should a solutions architect recommend?

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface
- B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface
- C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface
- D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface

Answer: D

Explanation:

Question: 205

A company is running a three-tier web application to process credit card payments. The front-end user interface consists of static webpages. The application tier can have long-running processes. The database tier uses MySQL. The application is currently running on a single general purpose large Amazon EC2 instance. A solutions architect needs to decouple the services to make the web application highly available. Which solution would provide the HIGHEST availability?

- A. Move static assets to Amazon CloudFront Leave the application in EC2 in an Auto Scaling group Move the database to Amazon RDS to deploy Multi-AZ
- B. Move static assets and the application into a medium EC2 instance Leave the database on me large instance Place both instances in an Auto Scaling group
- C. Move static assets to Amazon S3 Move the application to AWS Lambda with the concurrency limit set Move the database to Amazon DynamoDB with on-demand enabled
- D. Move static assets to Amazon S3 Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled Move the database to Amazon RDS to deploy Multi-AZ

Answer: D

Explanation:

Question: 206

A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data

a. The application cannot be modified to use any other communication protocols other than NFS for this purpose

Which storage solution should a solutions architect recommend for use after the migration?

- A. AWS DataSync
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon Elastic File System (Amazon EFS)
- D. Amazon EMR File System (Amazon EMRFS)

Answer: C

Explanation:

Question: 207

A company has an Amazon S3 bucket that contains confidential information in its production AWS account. The company has turned on AWS CloudTrail for the account. The account sends a copy of its logs to Amazon CloudWatch Logs. The company has configured the S3 bucket to log read and write data events.

A company auditor discovers that some objects in the S3 bucket have been deleted. A solutions architect must provide the auditor with information about who deleted the objects.

What should the solutions architect do to provide this information?

- A. Create a CloudWatch Logs filter to extract the S3 write API calls against the S3 bucket
- B. Query the CloudTrail logs with Amazon Athena to identify the S3 write API calls against the S3 bucket
- C. Use AWS Trusted Advisor to perform security checks for S3 write API calls that deleted the content
- D. Use AWS Config to track configuration changes on the S3 bucket. Use these details to track the S3 write API calls that deleted the content

Answer: B

Explanation:

Question: 208

A company has three AWS accounts Management Development and Production. These accounts use AWS services only in the us-east-1 Region All accounts have a VPC with VPC Flow Logs configured to publish data to an Amazon S3 bucket in each separate account For compliance reasons the company needs an ongoing method to aggregate all the VPC flow logs across all accounts into one destination S3 bucket in the Management account.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

- A. Add S3 Same-Region Replication rules in each S3 bucket that stores VPC flow logs to replicate objects to the destination S3 bucket Configure the destination S3 bucket to allow objects to be received from the S3 buckets in other accounts
- B. Set up an IAM user in the Management account Grant permissions to the IAM user to access the S3 buckets that contain the VPC flow logs Run the aws s3 sync command in the AWS CLI to copy the objects to the destination S3 bucket
- C. Use an S3 inventory report to specify which objects in the S3 buckets to copy Perform an S3 batch operation to copy the objects into the destination S3 bucket in the Management account with a single request.
- D. Create an AWS Lambda function in the Management account Grant S3 GET permissions on the source S3 buckets Grant S3 PUT permissions on the destination S3 bucket Configure the function to invoke when objects are loaded in the source S3 buckets

Answer: A

Explanation:

Question: 209

A company hosts an application on multiple Amazon EC2 instances The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.

What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue
- B. Use the Add Permission API call to add appropriate permissions
- C. Use the ReceiveMessage API call to set an appropriate wait time
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout

Answer: D

Explanation:

Question: 210

A company has an on-premises application that collects data and stores it to an on-premises NFS

server The company recently set up a 10 Gbps AWS Direct Connect connection The company is running out of storage capacity on premises. The company needs to migrate the application data from on premises to the AWS Cloud while maintaining low-latency access to the data from the on-premises application

What should a solutions architect do to meet these requirements?

- A. Deploy AWS Storage Gateway for the application data and use the file gateway to store the data in Amazon S3 Connect the on-premises application servers to the file gateway using NFS
- B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server and copy the application data to the EFS file system. Then connect the on-premises application to Amazon EFS
- C. Configure AWS Storage Gateway as a volume gateway Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots
- D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer Connect the on-premises application to the EFS file system

Answer: D

Explanation:

Question: 211

A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance Due to application limitations it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails

What would allow for automatic recovery of the EC2 instance as quickly as possible?

- A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired
- B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired
- C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired trigger instance recovery
- D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy

Answer: A

Explanation:

Question: 212

A company is running a multi-tier web application on AWS. The application runs its database on Amazon Aurora MySQL. The application and database tiers are in the us-east-1 Region.

A database administrator who monitors the Aurora DB cluster finds that an intermittent increase in read traffic is creating high CPU utilization on the read replica

- a. The result is increased read latency for the application. The memory and disk utilization of the DB

instance are stable throughout the event of increased latency.

What should a solutions architect do to improve the read scalability?

- A. Reboot the DB cluster
- B. Create a cross-Region read replica
- C. Configure Aurora Auto Scaling for the read replica
- D. Increase the provisioned read IOPS for the DB instance

Answer: B

Explanation:

Question: 213

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

- A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option
- B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot
- C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases
- D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances

Answer: A

Explanation:

Question: 214

A company wants to migrate its MySQL database from on-premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

- A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
- B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
- C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
- D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Answer: B

Explanation:

Question: 215

A company wants to perform an online migration of active datasets from an on-premises NFS server to an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. Data integrity verification is required during the transfer and at the end of the transfer. The data also must be encrypted.

A solutions architect is using an AWS solution to migrate the data.

Which solution meets these requirements?

- A. AWS Storage Gateway file gateway
- B. S3 Transfer Acceleration
- C. AWS DataSync
- D. AWS Snowball Edge Storage Optimized

Answer: C

Explanation:

Question: 216

A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML). The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region. The company hosts a web application that the customers use to purchase access to a given dataset. The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer. After a purchase is made, customers receive an S3 signed URL that allows access to the files.

The customers are distributed across North America and Europe. The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.

What should a solutions architect do to meet these requirements?

- A. Configure S3 Transfer Acceleration on the existing S3 bucket. Direct customer requests to the S3 Transfer Acceleration endpoint. Continue to use S3 signed URLs for access control.
- B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL. Switch to CloudFront signed URLs for access control.
- C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets. Direct customer requests to the closest Region. Continue to use S3 signed URLs for access control.
- D. Modify the web application to enable streaming of the datasets to end users. Configure the web application to read the data from the existing S3 bucket. Implement access control directly in the application.

Answer: B

Explanation:

Question: 217

A company stores user data in AWS. The data is used continuously with peak usage during business hours. Access patterns vary with some data not being used for months at a time. A solutions architect must choose a cost-effective solution that maintains the highest level of durability while maintaining high availability.

Which storage solution meets these requirements?

- A. Amazon S3 Standard
- B. Amazon S3 Intelligent-Tiering
- C. Amazon S3 Glacier Deep Archive
- D. Amazon S3 One Zone-infrequent Access (S3 One Zone-IA)

Answer: B

Explanation:

Question: 218

A developer is creating an AWS Lambda function to perform dynamic updates to a database when an item is added to an Amazon Simple Queue Service (Amazon SQS) queue. A solutions architect must recommend a solution that tracks any usage of database credentials in AWS CloudTrail. The solution also must provide auditing capabilities.

Which solution will meet these requirements?

- A. Store the encrypted credentials in a Lambda environment variable
- B. Create an Amazon DynamoDB table to store the credentials. Encrypt the table.
- C. Store the credentials as a secure string in AWS Systems Manager Parameter Store
- D. Use an AWS Key Management Service (AWS KMS) key store to store the credentials

Answer: D

Explanation:

Question: 219

A company has a service that reads and writes large amounts of data from an Amazon S3 bucket in the same AWS Region. The service is deployed on Amazon EC2 instances within the private subnet of a VPC. The service communicates with Amazon S3 over a NAT gateway in the public subnet. However, the company wants a solution that will reduce the data output costs.

Which solution will meet these requirements MOST cost-effectively?

- A. Provision a dedicated EC2 NAT instance in the public subnet. Configure the route table for the private subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
- B. Provision a dedicated EC2 NAT instance in the private subnet. Configure the route table for the public subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
- C. Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic.
- D. Provision a second NAT gateway. Configure the route table for the private subnet to use this NAT gateway as the destination for all S3 traffic.

Answer: C

Explanation:

Question: 220

A company has an application that uses an Amazon DynamoDB table for storage. A solutions architect discovers that many requests to the table are not returning the latest data.

a. The company's users have not reported any other issues with database performance. Latency is in an acceptable range.

Which design change should the solutions architect recommend?

- A. Add read replicas to the table.
- B. Use a global secondary index (GSI).
- C. Request strongly consistent reads for the table.
- D. Request eventually consistent reads for the table.

Answer: C

Explanation:

Question: 221

A company wants to share data that is collected from self-driving cars with the automobile community. The data will be made available from within an Amazon S3 bucket. The company wants to minimize its cost of making this data available to other AWS accounts.

What should a solutions architect do to accomplish this goal?

- A. Create an S3 VPC endpoint for the bucket.
- B. Configure the S3 bucket to be a Requester Pays bucket.
- C. Create an Amazon CloudFront distribution in front of the S3 bucket.
- D. Require that the files be accessible only with the use of the BitTorrent protocol.

Answer: A

Explanation:

Question: 222

A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.

The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.

Which combination of actions should a solutions architect take to meet these requirements? (Select TWO.)

- A. Configure Amazon CloudFront to cache multiple versions of the content.
- B. Configure a host header in a Network Load Balancer to forward traffic to different instances.

- C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.
- D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.
- E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Answer: B, D

Explanation:

Question: 223

An airline that is based in the United States provides services for routes in North America and Europe. The airline is developing a new read-intensive application that customers can use to find flights on either continent.

The application requires strong read consistency and needs scalable database capacity to accommodate changes in user demand. The airline needs the database service to synchronize with the least possible latency between the two continents and to provide a simple failover mechanism to a second AWS Region.

Which solution will meet these requirements?

- A. Deploy Microsoft SQL Server on Amazon EC2 instances in a Region in North America. Use SQL Server binary log replication on an EC2 instance in a Region in Europe.
- B. Create an Amazon DynamoDB global table. Add a Region from North America and a Region from Europe to the table. Query data with strongly consistent reads.
- C. Use an Amazon Aurora MySQL global database. Deploy the read-write node in a Region in North America, and deploy read-only endpoints in Regions in North America and Europe. Query data with global read consistency.
- D. Create a subscriber application that uses Amazon Kinesis Data Streams for an Amazon Redshift cluster in a Region in North America. Create a second subscriber application for the Amazon Redshift cluster in a Region in Europe. Process all database modifications through Kinesis Data Streams.

Answer: C

Explanation:

Question: 224

A company has a production web application in which users upload documents through a web interlace or a mobile app. According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

- A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled
- B. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.
- C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an

ACL to restrict all access to read-only.

D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

Answer: A

Explanation:

Question: 225

A company has a Microsoft NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.

Which combination of actions should the company take to meet these requirements? (Select TWO.)

- A. Refactor the application as serverless with AWS Lambda functions running NET Core.
- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI).
- D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Answer: A, D

Explanation:

Question: 226

A company wants to enforce strict security guidelines on accessing AWS Cloud resources as the company migrates production workloads from its data centers. Company management wants all users to receive permissions according to their job roles and functions.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an AWS Single Sign-On deployment. Connect to the on-premises Active Directory to centrally manage users and permissions across the company
- B. Create an IAM role for each job function. Require each employee to call the sts:AssumeRole action in the AWS Management Console to perform their job role.
- C. Create individual IAM user accounts for each employee. Create an IAM policy for each job function, and attach the policy to all IAM users based on their job role.
- D. Create individual IAM user accounts for each employee. Create IAM policies for each job function. Create IAM groups, and attach associated policies to each group. Assign the IAM users to a group based on their Job role.

Answer: D

Explanation:

Question: 227

A company provides machine learning solutions. The company's users need to download large data sets from the company's Amazon S3 bucket. These downloads often take a long time, especially when the users are running many simulations on a subset of those datasets. Users download the datasets to Amazon EC2 instances in the same AWS Region as the S3 bucket. Multiple users typically use the same datasets at the same time.

Which solution will reduce the time that is required to access the datasets?

- A. Configure the S3 bucket to use the S3 Standard storage class with S3 Transfer Acceleration activated.
- B. Configure the S3 bucket to use the S3 Intelligent-Tiering storage class with S3 Transfer Acceleration activated.
- C. Create an Amazon Elastic File System (Amazon EFS) network file system. Migrate the datasets by using AWS DataSync.
- D. Move the datasets onto a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Attach the volume to all the EC2 instances.

Answer: C

Explanation:

Question: 228

A company needs to retain its AWS CloudTrail logs (for 3 years). The company is enforcing CloudTrail across a set of AWS accounts by using AWS Organizations from the parent account. The CloudTrail target S3 bucket is configured with S3 Versioning enabled. An S3 Lifecycle policy is in place to delete current objects after 3 years.

After the fourth year of use of the S3 bucket, the S3 bucket metrics show that the number of objects has continued to rise. However, the number of new CloudTrail logs that are delivered to the S3 bucket has remained consistent.

Which solution will delete objects that are older than 3 years in the MOST cost-effective manner?

- A. Configure the organization's centralized CloudTrail trail to expire objects after 3 years.
- B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.
- C. Create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years.
- D. Configure the parent account as the owner of all objects that are delivered to the S3 bucket.

Answer: B

Explanation:

Question: 229

A company has a website hosted on AWS. The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS.

What should a solutions architect do to meet this requirement?

- A. Update the ALB's network ACL to accept only HTTPS traffic
- B. Create a rule that replaces the HTTP in the URL with HTTPS.
- C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
- D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Answer: C

Explanation:

Question: 230

A company is deploying an application that processes large quantities of data in batches as needed. The company plans to use Amazon EC2 instances for the workload. The network architecture must support a highly scalable solution and prevent groups of nodes from sharing the same underlying hardware.

Which combination of network solutions will meet these requirements? (Select TWO.)

- A. Create Capacity Reservations for the EC2 instances to run in a placement group
- B. Run the EC2 instances in a spread placement group.
- C. Run the EC2 instances in a cluster placement group.
- D. Place the EC2 instances in an EC2 Auto Scaling group.
- E. Run the EC2 instances in a partition placement group.

Answer: B, C

Explanation:

Question: 231

A company is planning to store sensitive documents in an Amazon S3 bucket. The documents must be encrypted at rest. The company wants to manage the underlying keys that are used for encryption. However, the company does not want to manage the encryption and decryption process. Which solutions will meet these requirements? (Select TWO.)

- A. Use server-side encryption with customer-provided encryption keys (SSE-C).
- B. Use client-side encryption with AWS managed keys.
- C. Use server-side encryption with S3 managed encryption keys (SSE-S3).
- D. Use server-side encryption with AWS KMS managed encryption keys (SSE-KMS) with a key policy document that is 40 KB in size
- E. Use server-side encryption with AWS KMS managed encryption keys (SSE-KMS) that the company uploads to AWS KMS.

Answer: C, E

Explanation:

Question: 232

A company has an Amazon S3 bucket that contains mission-critical data.

a. The company wants to ensure this data is protected from accidental deletion. The data should still be accessible, and a user should be able to delete the data internationally.

Which combination of steps should a solutions architect take to accomplish this? (Select TWO.)

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.
- C. Create a bucket policy on the S3 bucket.
- D. Enable default encryption on the S3 bucket.
- E. Create a lifecycle policy for the objects in the S3 bucket.

Answer: A, B

Explanation:

Question: 233

A company build an application that gives users the ability to check in to places they visit, rank the places, and add reviews about their experiences. The application is successful and is experiencing a rapid increase in the number of users every month.

The company uses a single Amazon RDS for MySQL DB instance for its database. The company fears that the database might not be able to handle the load for the upcoming month because the DB instance has activated alarms that are related to resource exhaustion.

A solutions architect must design a solution that prevents service interruptions at the database layer. The solutions architect also must minimize any changes to code.

Which solution meets these requirements?

- A. Create RDS read replicas. Redirect read-only traffic to the read replica endpoints.
- B. Create an Amazon EMR cluster. Migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.
- C. Create an Amazon ElastiCache cluster. Redirect all read-only traffic to the cluster. Set up the cluster to be deployed in three Availability Zones.
- D. Turn on the Multi-AZ feature for the DB instance. Redirect read-only traffic to the standby replica endpoint.

Answer: A

Explanation:

Question: 234

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products.

What should a solutions architect recommend to ensure that all the requests are processed successfully?

- A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
- B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
- C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
- D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

Answer: D

Explanation:

Question: 235

A disaster relief company is designing a new solution to analyze real-time csv data

a. The data is collected by a network of thousands of research stations and is distributed across the world. The data volume is consistent and constant, and the size of each data file is 512 KB. The company needs to stream the data and analyze the data in real time.

Which combination of actions should a solutions architect take to meet these requirements? (Select TWO.)

- A. Provision an appropriately sized Amazon Simple Queue Service (Amazon SQS) queue. Use the AWS SDK at the research stations to write the data into the SQS queue
- B. Provision an appropriately sized Amazon Kinesis Data Firehose delivery stream. Use the AWS SDK at the research stations to write the data into the delivery stream and then into an Amazon S3 bucket.
- C. Provision an appropriately sized Amazon Kinesis Data Analytics application. Use the AWS CLI to configure Kinesis Data Analytics with SQL queries
- D. Provision an AWS Lambda function to process the data. Set up the BatchSize property on the Lambda event source.
- E. Provision an AWS Lambda function to process the data. Set up an Amazon EventBridge (Amazon CloudWatch Events) cron expression rule to invoke the Lambda function

Answer: A, D

Explanation:

Question: 236

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics
- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis

- C. Cache the data to Amazon CloudFront: Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
- D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Answer: D

Explanation:

Topic 3, Exam Pool C

Question: 237

A company runs an application in the AWS Cloud and uses Amazon DynamoDB as the database. The company deploys Amazon EC2 instances to a private network to process data from the database. The company uses two NAT instances to provide connectivity to DynamoDB. The company wants to retire the NAT instances. A solutions architect must implement a solution that provides connectivity to DynamoDB and that does not require ongoing management. What is the MOST cost-effective solution that meets these requirements?

- A. Create a gateway VPC endpoint to provide connectivity to DynamoDB.
- B. Configure a managed NAT gateway to provide connectivity to DynamoDB.
- C. Establish an AWS Direct Connect connection between the private network and DynamoDB.
- D. Deploy an AWS PrivateLink endpoint service between the private network and DynamoDB.

Answer: A

Explanation:

Question: 238

An entertainment company is using Amazon DynamoDB to store media metadata. The application is read-intensive and experiences delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application. What should a solutions architect recommend to meet this requirement?

- A. Use Amazon ElastiCache for Redis.
- B. Use Amazon DynamoDB Accelerator (DAX).
- C. Replicate data by using DynamoDB global tables.
- D. Use Amazon ElastiCache for Memcached with AutoDiscovery enabled.

Answer: B

Explanation:

Question: 239

A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years.

before they can be deleted Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days

Which storage solution is MOST cost-effective?

- A. Create an S3 bucket lifecycle policy to move Mm from S3 Standard to S3 Glacier 30 days from object creation Delete the Tiles 4 years after object creation
- B. Create an S3 bucket lifecycle policy to move tiles from S3 Standard to S3 One Zone-infrequent Access (S3 One Zone-IA) 30 days from object creation. Delete the fees 4 years after object creation
- C. Create an S3 bucket lifecycle policy to move files from S3 Standard-infrequent Access (S3 Standard-IA) 30 from object creation. Delete the ties 4 years after object creation
- D. Create an S3 bucket Lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation Move the files to S3 Glacier 4 years after object carton.

Answer: C

Explanation:

Question: 240

A company develops web applications. As part of its development process, the company constantly launches and deletes Application Load Balancers (ALBs) in multiple AWS Regions.

The company wants to create an allow list on its firewall device. The allow list will contain the IP addresses of an the load balancers. A solutions architect needs a one-line, highly available solution that will accomplish that goal and will help reduce the number of IP addresses that the firewall needs to allow.

Which solution will meet these requirements with the LEAST amount of operational overhead?

- A. Create an AWS Lambda function to keep track of the IP addressee tor al the ALBs in different Regions. Keep refreshing this list.
- B. Set up a Network Load Balancer (NLB) with Elastic IP addresses Register the private IP addresses of all the ALBs as targets for the NLB
- C. Launch AWS Global Accelerator Create endpoints for each of the Regions that are m use. Register all the ALBs in the Regions to the corresponding endpoints.
- D. Set up an Amazon EC2 Instance Assign an Elastic IP address to the EC2 instance. Configure the EC2 instance as a proxy to forward traffic to all the ALBs

Answer: C

Explanation:

Question: 241

A company hosts a popular website in the AWS Cloud, A solutions architect needs to provide reports about user click behaviour in near-real time as users navigate the website.

Which solution will meet this requirement

- A. Store the clickstream data in Amazon DynamoDB. Deploy an application that runs on AWS Elastic

Beantalk to process and analyze the data.

B. Push the clickstream data from each session to an Amazon Kinesis data stream Analyze the data by using Amazon Kinesis Data Analytics.

C. Store the clickstream data in an Amazon S3 bucket. Order the data by timestamp Process the data with an AWS Lambda function that is subscribed to object creation events on the S3 bucket.

D. Forward the clickstream data to Amazon Simple Queue Service (Amazon SQS) Store the data in an Amazon RDS for MySQL DB instance. Deploy Amazon EC2 Instances to process and analyze the data

Answer: B

Explanation:

Question: 242

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Select TWO.)

A. Configure storage Auto Scaling on the RDS for Oracle Instance.

B. Migrate the database to Amazon Aurora to use Auto Scaling storage.

C. Configure an alarm on the RDS for Oracle Instance for low free storage space

D. Configure the Auto Scaling group to use the average CPU as the scaling metric

E. Configure the Auto Scaling group to use the average free memory as the scaling metric

Answer: A, C

Explanation:

Question: 243

A company plans to host a survey website on AWS. The company anticipates an unpredictable amount of traffic. This traffic results in asynchronous updates to the database. The company wants to ensure that writes to the database hosted on AWS do not get dropped. How should the company write its application to handle these database requests?

A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.

B. Configure the application to subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Publish the database updates to the SNS topic

C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the database connection until the database has resources to write the data.

D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues for capturing the writes and draining the queue as each write is made to the database.

Answer: D

Explanation:

Question: 244

A database is on an Amazon RDS MySQL 5.6 Multi-AZ DB instance that experiences highly dynamic reads. Application developers notice a significant slowdown when testing read performance from a secondary AWS Region. The developers want a solution that provides less than 1 second of read replication latency.

What should the solutions architect recommend?

- A. Install MySQL on Amazon EC2 in the secondary Region
- B. Migrate the database to Amazon Aurora with cross-Region replicas.
- C. Create another RDS for MySQL read replica in the secondary Region
- D. Implement Amazon ElastiCache to improve database query performance

Answer: B

Explanation:

Question: 245

A company stores recordings on a monthly basis. Users access the recordings randomly within 1 year of recording, but users rarely access the files after 1 year. The company wants to optimize its solution by allowing only files that are newer than 1 year old to be queried and retrieved as quickly as possible. A delay in retrieving older files is acceptable.

Which solution meets these requirements MOST cost-effectively?

- A. Store individual files in Amazon S3. Store search metadata in object tags that are created in S3. Query the S3 tags to retrieve the files from S3.
- B. Store individual files in Amazon S3. Use S3 Lifecycle policies to move the files to S3 Glacier after 1 year. Query and retrieve the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.
- C. Store individual files in Amazon S3. Store search metadata for each archive in Amazon S3. Use S3 Lifecycle policies to move the files to S3 Glacier after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
- D. Store individual files in Amazon S3. Use S3 Lifecycle policies to move the files to S3 Glacier after 1 year. Store search metadata in Amazon RDS. Query the metadata from Amazon RDS. Retrieve the files from Amazon S3 or S3 Glacier.

Answer: D

Explanation:

Question: 246

A company is using a VPC peering strategy to connect its VPCs in a single Region to allow for cross-

communication. A recent increase in account creations and VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs. There are also new requests to create site-to-site VPNs some of the VPCs. A solution architect has been tasked with creating a centrally managed networking setup for multiple account, VPCs and VPNs. Which networking solution these requirements?

- A. Configure shared VPCs and VPNs and share to each other.
- B. Configure a hub-and-spoke VPC and route all traffic through VPC peering.
- C. Configure an AWS Direct Connect connection between al VPCs and VPNs.
- D. Configure a transit gateway with Transit Gateway and connect all VPCs and VPNs.

Answer: D

Explanation:

Question: 247

A company uses a combination of Amazon EC2 instances and AWS Fargate tasks to process daily transactions. The company faces unpredictable and sudden increases in transaction volume. The company needs a solution that will process the transactions immediately. Which solution meets these requirement MOST cost-effectively?

- A. Purchase a Compute Savings Plan
- B. Purchase an EC2 Instance Savings Plan.
- C. Purchase Reserved Instances tor existing EC2 workloads.
- D. Use Spot Instances for existing EC2 workloads.
- E. Use Far gale Spot capacity for thetasks.

Answer: B

Explanation:

Question: 248

A company's web application is running on Amazon EC2 instances behind an application Load Balancer. The company changed its policy., which now requires the application to be accessed from one specific country only. Which configuration will meet this requirement?

- A. Configure the security group for the EC2 Instances
- B. Configure the security group on the Application Load Balancer
- C. Configure AWS WAF on the Application Load Balancer in a VPC
- D. Configure the network ACL for the subnet that contains the EC2 instances

Answer: C

Explanation:

Question: 249

A company has a web server running on an Amazon EC2 instance in public subnet with an Elastic IP address. The default security group is assigned to the EC2 instances. The default network ACL has been modified to block all traffic. A solution architect needs to make the web server accessible from everywhere on port 443.

Which combination of steps will accomplish this task? (Select TWO)

- A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0
- B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
- C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
- D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
- E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32766-65535 to destination 0.0.0.0/0

Answer: A, E

Explanation:

Question: 250

A company requires that all version of object in its Amazon S3 bucket be retained. Current object versions will be frequently accessed during the first 30 days, after which they will be rarely accessed and must be retrievable within 5 minutes. Previous object versions need to be kept forever, will be rarely accessed, and can be retrieved within 1 week. All store solutions must be highly available and highly durable

What should a solutions architect recommend to meet these requirements in the MOST cost-effective manner?

- A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day
- B. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- C. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 standard-infrequent Access (S3 Standard-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- D. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day

Answer: B

Explanation:

Question: 251

At part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solution architect needs to determine the most

efficient way to obtain this report Information

Which solution meets these requirement?

- A. Run a query with Amazon Athena to generate the report.
- B. Create a report in Cost Explorer and download the report
- C. Access the bill details from the tuning dashboard and download via bill.
- D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Answer: B

Explanation:

Question: 252

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want the new service to affect the performance of the current application. What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Answer: C

Explanation:

Question: 253

A company is hosting its website by using Amazon EC2 instances behind an Elastic Load balancer across multiple Availability Zones. The instances run in an EC2 Scaling group. The website uses Amazon Elastic Block Store (Amazon EBS) volume to store product manuals for users to download. The company updates the product content often, so new instances launched by the Auto Scaling group often have data

a. It can take up to 30 minutes for the new instances to receive all the updates. The updates also require the EBS volumes to be resized during business hours.

The company wants to ensure that the product manuals are always up to date on all instances and that the architecture adjusts quickly to increased user demand. A solutions architect needs to meet these requirements without causing the company to update its application code or adjust its website. What should the solutions architect do to accomplish this goal?

- A. Store the product manuals in an EBS volume mount that volume to the EC2 instances

- B. Store the product manuals in an Amazon S3 bucket Redirect the downloads to this bucket
- C. Store the product manuals in an Amazon Elastic File System (Amazon EFS) volume. Mount that volume to the EC2 instances
- D. Store the product manuals in an Amazon S3 Standard-Infrequent Access (S3 Standard-IA) bucket. Redirect the downloads to this bucket

Answer: C

Explanation:

Question: 254

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in a very AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

- A. Configure an accelerator in AWS Global Accelerator. Add listeners for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behaviour to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behaviour to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

Answer: A

Explanation:

Question: 255

A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested that the solutions architect design a solution to move existing data and support future records.

Which services can the solutions architect recommend to meet these requirements?

- A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data.

Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
D. Use AWS Storage Gateway to move existing data to AWS Use Amazon Elastic Block Stores (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging

Answer: A

Explanation:

Question: 256

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents. Which combination of actions should be taken to meet these requirements? (Select TWO.)

- A. Enable a read-only bucket ACL
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Answer: B, D

Explanation:

Question: 257

A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3.
Which solution meets these requirements and is MOST cost-effective?

- A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.
- B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3
- C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on-premises to Amazon S3
- D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3

Answer: B

Explanation:

Question: 258

A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider to authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that are stored in another S3 bucket.
Upon deployment of the application, users report errors and are unable to access the protected content. A solutions architect must resolve this issue by providing proper permissions so that users

can access the protected content.

Which solution meets these requirements?

- A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.
- B. Update the S3 ACL to allow the application to access the protected content
- C. Redeploy the application to Amazon S3 to prevent eventually consistent reads in the S3 bucket from affecting the ability of users to access the protected content.
- D. Update the Amazon Cognito pool to use custom attribute mappings within the Identity pool and grant users the proper permissions to access the protected content

Answer: B

Explanation:

Question: 259

A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly. Currently subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.

What should a solutions architect do to optimize costs?

- A. Create an additional NAT gateway. Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic
- B. Create an internet gateway. Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic
- C. Create a VPC endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint.
- D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

Answer: C

Explanation:

Question: 260

A company needs to save the results from a medical trial to an Amazon S3 repository. The repository must allow a few scientists to add new files and must restrict all other users to read-only access. No users can have the ability to modify or delete any files in the repository. The company must keep every file in the repository for a minimum of 1 year after its creation date.

Which solution will meet these requirements?

- A. Use S3 Object Lock in governance mode with a legal hold of 1 year
- B. Use S3 Object Lock in compliance mode with a retention period of 365 days.
- C. Use an IAM role to restrict all users from deleting or changing objects in the S3 bucket. Use an S3 bucket policy to only allow the IAM role

D. Configure the S3 bucket to invoke an AWS Lambda function every time an object is added. Configure the function to track the hash of the saved object so that modified objects can be marked accordingly.

Answer: B

Explanation:

Question: 261

A company is rebuilding its data center and wants to securely transfer 50 TB of data to AWS within 2 weeks. The existing data center has a Site-to-Site VPN connection to AWS that is 90% utilized. Which AWS service should a solutions architect use to meet these requirements?

- A. AWS DataSync with a VPC endpoint
- B. AWS Direct Connect
- C. AWS Snowball Edge Storage Optimized
- D. AWS Storage Gateway

Answer: C

Explanation:

Question: 262

A company wants to move a multi-tiered application from on-premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of REST APIs. Which solution meets these needs and is the MOST operationally efficient?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the servers' peak utilization during the performance failures. Increase the size of the application servers' Amazon EC2 instance to meet the peak requirements.
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Answer: D

Explanation:

Question: 263

A company runs an internet-facing web application on AWS. The company uses Amazon Route 53 for DNS management and has a public hosted zone to route traffic from the internet to the application. The company wants to log DNS response codes to help system administrators perform any root cause analysis in the future.

Which solution will meet these requirements?

- A. Use Route 53 to configure query logging
- B. Use AWS CloudTrail to record all Route 53 queries
- C. Use Amazon CloudWatch to record and process Route 53 metrics
- D. Use AWS Trusted Advisor to perform on-demand root cause analysis

Answer: A

Explanation:

Question: 264

A company wants to migrate its accounting system from an on-premises data center to the AWS Cloud in a single AWS Region. Data security and an immutable audit log are the top priorities. The company must monitor all AWS activities for compliance auditing. The company that enabled AWS CloudTrail but wants to make sure it meets all requirements. Which actions should a solutions architect take to protect and secure CloudTrail? (Select TWO.)

- A. Enable CloudTrail log file validation.
- B. Enable the CloudTrail Proceeding Library.
- C. Enable logging of Insights events in CloudTrail.
- D. Enable custom logging from the on-premises resources
- E. Create an AWS Config rule to monitor whether CloudTrail is configured to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS)

Answer: A, E

Explanation:

Question: 265

A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.

What should the solution architect do to accomplish this?

- A. Provide an API hosted on an Amazon EC2 Instance. The EC2 instance performs the required computations when the API request is made.
- B. Design a REST API using Amazon API Gateway that accepts the item names API Gateway passes item names to AWS Lambda for tax computations
- C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
- D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2

instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations

Answer: B

Explanation:

Question: 266

A company uses Amazon Redshift for to data warehouse. The company wants to ensure high durability for its data in case of any component failure. What should a solution architect recommend?

- A. Enable concurrency scaling
- B. Enable cross-Region snapshots
- C. Increase the data retention period
- D. Deploy Amazon Redshift in Multi-AZ

Answer: D

Explanation:

Question: 267

A company used an AWS Direct Connect connection to copy 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region. The company now wants to copy the data to another S3 bucket in the us-west-2 Region. Which solution will meet this requirement?

- A. Use an AWS Snowball Edge Storage Optimized device to copy the data from the colocation facility to us-west-2
- B. Use the S3 console to copy the data from the source S3 bucket to the target S3 bucket.
- C. Use S3 Transfer Acceleration and the S3 copy-object command to copy the data from the source S3 bucket to the target S3 bucket
- D. Add an S3 Cross-Region Replication configuration to copy the data from the source S3 bucket to the target S3 bucket.

Answer: D

Explanation:

Question: 268

A solution architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently the day. An Application load balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed. What should the solutions architect do to ensure that the architecture supports distributed session

data management?

- A. Use Amazon ElastiCache to manage and store session data.
- B. Use session affinity (sticky sessions) of the ALB to manage session data.
- C. Use Session Manager from AWS Systems Manager to manage the session.
- D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session.

Answer: C

Explanation:

Question: 269

A company uses an application to present metrics from sporting events to the public. The application must scale quickly during live events and must store these metrics for long-term reporting purposes. The company's architecture includes the following:

- * Amazon EC2 instances that run in an Auto Scaling group in private subnets
- * A network Load Balancer That runs in public subnets
- * A MongoDB database cluster that runs across multiple EC2 instances

A solutions architect must implement a solution that minimizes operational overhead. The solution also must be able to scale automatically. What should the solutions architect set up to meet these requirements?

- A. An Amazon DynamoDB database
- B. An Amazon RDS for MySQL DB instance
- C. EC2 instances that run MySQL
- D. Amazon Redshift

Answer: A

Explanation:

Question: 270

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10GB in size. The application owner will make the log file available to the vendor for a limited time.

What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor
- B. Upload the log to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multifactor authentication

Answer: C

Explanation:

Question: 271

Some of the company's customers are retrieving records frequently, leading to an increase in costs for the company. The company wants to limit retrieved requests in the future. The company also wants to ensure that if one customer reaches its retrieval limit other customers will not be affected. Which solution will meet these requirements?

- A. Set up server-side throttling limits for API Gateway.
- B. Limit DynamoDB read throughput on the table to an amount that results in the maximum cost that the company is willing to incur.
- C. Set up a usage plan for API Gateway. Implement throttling limits for each customer, and distribute API keys to each customer.
- D. Set up AWS Budgets. Monitor the usage of API Gateway and DynamoDB. Configure an alarm to provide an alert when the cost exceeds a certain threshold each month.

Answer: D

Explanation:

Question: 272

A company runs an application on Amazon EC2 instances backed by Amazon Elastic Block Store (Amazon EBS). The instances need to be available for 12 hours daily. The company wants to save costs by making the instance unavailable outside the window required for the application. However, the contents of the memory must be preserved whenever the instance is unavailable. What should a solutions architect do to meet this requirement?

- A. Stop the instance outside the application's availability window. Start up the instance again when required.
- B. Hibernate the instance outside the application's availability window. Start up the instance again when required.
- C. Use Auto Scaling to scale down the instance outside the application's availability window. Scale up the instance when required.
- D. Terminate the instance outside the application's availability window. Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

Answer: A

Explanation:

Question: 273

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases. Which solution meets these requirements?

- A. Enable a Multi-AZ deployment for the DB instance.

- B. Enable auto scaling for the OB instance in one Availability Zone.
- C. Configure the OB instance in one Availability Zone and create multiple read replicas in a separate Availability Zone
- D. Configure the OB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks

Answer: A

Explanation:

Question: 274

A company is running an application on AWS to process weather sensor data that is stored in an Amazon S3 bucket. Three batch jobs run hourly to process the data in the S3 bucket for different purposes. The company wants to reduce the overall processing time by running the three applications in parallel using an event-based approach.

What should a solutions architect do to meet these requirements?

- A. Enable S3 Event Notifications for new objects to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Subscribe all applications to the queue for processing.
- B. Enable S3 Event Notifications for new objects to an Amazon Simple Queue Service (Amazon SQS) standard queue. Create an additional SQS queue for all applications, and subscribe all applications to the standard queue for processing.
- C. Enable S3 Event Notifications for new objects to separate Amazon Simple Queue Service (Amazon SQS) FIFO queues. Create an additional SQS queue (one for each application) and subscribe each queue to the initial topic for processing.
- D. Enable S3 Event Notifications for new objects to an Amazon Simple Notification Service (Amazon SNS) topic. Create an Amazon Simple Queue Service (Amazon SQS) queue for each application, and subscribe each queue to the topic for processing.

Answer: D

Explanation:

Question: 275

A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so.

How should a solutions architect provide access to the SQS queue?

- A. Create an Instance profile that provides the other company access to the SQS queue
- B. Create an IAM policy that provides the other company access to the SQS queue.
- C. Create an SQS access policy that provides the other company access to the SQS queue
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic policy that provides the other company access to the SQS queue

Answer: C

Explanation:

Question: 276

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

- A. Enable the versioning and MFA Delete features on the S3 bucket.
- B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
- C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3 DeleteObject action during audit dates.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Answer: A

Explanation:

Question: 277

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.

Which service should a solutions architect recommend?

- A. Amazon Aurora MySQL
- B. Amazon Aurora Serverless for MySQL
- C. Amazon Redshift Spectrum
- D. Amazon RDS for MySQL

Answer: B

Explanation:

Question: 278

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meets these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.

- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: B

Explanation:

Question: 279

A company wants to use an AWS Region as a disaster recovery location for its on-premises infrastructure. The company has 10 TB of existing data and the on-premises data center has a 1Gbps internet connection. A solution architect must find a solution so the company can have its existing data on AWS in 72 hours without transmitting it using an unencrypted channel.

Which solution should the solutions architect select?

- A. Send the initial 10 TB of data to AWS using FTP.
- B. Send the initial 10 TB of data to AWS using AWS Snowball.
- C. Establish a VPN connection between Amazon VPC and the company's data center.
- D. Establish an AWS Direct Connect connection between Amazon VPC and the company's data center.

Answer: C

Explanation:

Q: How long does it take to transfer my data?

Data transfer speed is affected by a number of factors including local network speed, file size, and the speed at which data can be read from your local servers. The end-to-end time to transfer up to 80 TB of data into AWS with Snowball Edge is approximately one week, including the usual shipping and handling time in AWS data centers.

Q: How quickly can I access my exported data?

We typically start exporting your data within 24 hours of receiving your request, and exporting data can take as long as a week. Once the job is complete and the device is ready, we ship it to you using the shipping options you selected when you created the job.

(Source: <https://aws.amazon.com/snowball/fags/>)

Question: 280

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

Answer: B

Explanation:

Question: 281

A company collects 10 GB of telemetry data daily from various machines. The company stores the data in an Amazon S3 bucket in a source data account.

The company has hired several consuming agencies to use this data for analysis. Each agency needs read access to the data for its analysis. The company must share the data from the source data account by choosing a solution that maximizes security and operational efficiency. Which solution will meet these requirements?

- A. Configure S3 global tables to replicate data for each agency
- B. Make the S3 bucket public for a limited time Inform only the agencies
- C. Configure cross-account access for the S3 bucket to the accounts that the agencies own.
- D. Set up an IAM user for each analyst in the source data account Grant each user access to the S3 bucket

Answer: A

Explanation:

Question: 282

A company has primary and secondary data centers that are 500 miles (804.7 km) apart and interconnected with high-speed fiber-optic cable. The company needs a highly available and secure network connection between its data centers and a VPC on AWS for a mission-critical workload. A solutions architect must choose a connection solution that provides maximum resiliency. Which solution meets these requirements?

- A. Two AWS Direct Connect connections from the primary data center terminating at two Direct Connect locations on two separate devices
- B. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on the same device
- C. Two AWS Direct Connect connections from each of the primary and secondary data centers terminating at two Direct Connect locations on two separate devices
- D. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on two separate devices

Answer: C

Explanation:

Question: 283

A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.

What should a solutions architect do to meet this requirement?

- A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer.
- B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region
- C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application.
- D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer.

Answer: A

Explanation:

Question: 284

A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account. Which solution will meet these requirement in the MOST secure manner?

- A. Apply an S3 bucket policy that grants read access to the S3 bucket
- B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket
- C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket
- D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account

Answer: B

Explanation:

Question: 285

A company has a corporate network on premises and has three VPCs in the AWS Cloud. The company has one VPC each for development, test, and, production. The company wants its system administrators to securely gain remote command-line access from the corporate network to Amazon EC2 instances in the VPCs.

Which solution meets these requirements MOST cost-effectively?

- A. Set up a VPN connection between the corporate network and each of the three VPCs by using AWS VPN. Use Remote Desktop Protocol (RDP) or SSH over the VPN connection to access the EC2 instances remotely.

- B. Configure the EC2 instances to use an instance profile that trusts AWS Systems Manager Use Systems Manager Session Manager to gain console access to the EC2 instances
- C. Create a new VPC Purchase and install a virtual router from AWS Marketplace Establish a VPN connection from the corporate network to this router. Establish another VPN connection from the 'outer to the other three VPCs Use Remote Desktop Protocol (RDP) or SSH over the VPN connection to access the EC2 instances remotely.
- D. Create a new VPC Establish a VPN connection to the new VPC. Configure peering connections between the new VPC and the existing VPCs In the new VPC create an EC2 bastion host to serve as a jump box to EC2 instances in the other VPCs Use Remote Desktop Protocol (RDP) or SSH over the VPN connection to the bastion host

Answer: A

Explanation:

Question: 286

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable internet access for the private subnets?

- A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
- B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
- C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private Internet gateway.
- D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress-only internet gateway.

Answer: A

Explanation:

Question: 287

A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.

- A. Attach a resource-based policy to the S3 bucket
- B. Create an IAM user for the application with specific permissions to the S3 bucket
- C. Associate an IAM role with least privilege permissions to the EC2 instance profile
- D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls

Answer: C

Explanation:

Question: 288

A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users. The volume of requests is highly variable: several hours can pass without receiving a single request. The data processing will take place asynchronously, but should be completed within a few seconds after a request is made.

Which compute service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?

- A. An AWS Glue job
- B. An AWS Lambda function
- C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)
- D. A containerized service hosted in Amazon ECS with Amazon EC2

Answer: C

Explanation:

Question: 289

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

- A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.
- B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
- C. Store ingested data in an EC2 instance. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
- D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

Answer: A

Explanation:

Question: 290

A company is running a multi-tier recommendation web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the

application during periods high demand.

A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20.000.

What should a solutions architect do to improve the application performance?

- A. Replace the volume with a magnetic volume.
- B. Increase the number of IOPS on the gp3 volume.
- C. Replace the volume with a Provisioned IOPS SSD (Io2) volume.
- D. Replace the 2.000 GB gp3 volume with two 1.000 GB gp3 volumes

Answer: C

Explanation:

Question: 291

A news company that has reporters all over the world is hosting its broadcast system on AWS. The reporters send live broadcasts to the broadcast system. The reporters use software on their phones to send live streams through the Real Time Messaging Protocol (RTMP).

A solutions architect must design a solution that gives the reporters the ability to send the highest quality streams. The solution must provide accelerated TCP connections back to the broadcast system.

What should the solutions architect use to meet these requirements?

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. AWS Client VPN
- D. Amazon EC2 Instances and AWS Elastic IP addresses

Answer: B

Explanation:

Question: 292

A company runs its Infrastructure on AWS and has a registered base of 700.000 users for a document management application. The company intends to create a product that converts large pdf files to jpg image files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over time.

Which solution meets these requirements MOST cost-effectively?

- A. Save the pdf files to Amazon S3. Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to jpg format and store them back in Amazon S3.
- B. Save the pdf files to Amazon DynamoDB. Use the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to jpg format and store them back in DynamoDB.
- C. Upload the pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic Block Store (Amazon EBS) storage and an Auto Scaling group. Use a program in the

EC2 instances to convert the files to jpg format Save the .pdf files and the .jpg files In the EBS store.
D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to jpg format Save the pdf files and the jpg files in the EBS store.

Answer: D

Explanation:

Question: 293

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity
Which architecture offers the HIGHEST availability?

- A. Add a second ActiveMQ server to another Availability Zone Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- B. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.
- D. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS (or MySQL with Multi-AZ enabled).

Answer: D

Explanation:

Question: 294

A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.

A solutions architect needs to design a network connectivity solution that maximizes cost-effectiveness.

Which solution meets these requirements?

- A. Configure three AWS Site-to-Site VPN connections from the data center to AWS. Establish connectivity by configuring one VPN connection for each VPC.
- B. Launch a third-party virtual network appliance in each VPC. Establish an IPsec VPN tunnel between the data center and each virtual appliance.
- C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway In

us-east-1. Establish connectivity by configuring each VPC to use one of the Direct Connect connections.

D. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

Answer: C

Explanation:

Question: 295

A law firm needs to share information with the public. The information includes hundreds of files that must be publicly readable. Modifications or deletions of the files by anyone before a designated future date are prohibited.

Which solution will meet these requirements in the MOST secure way?

- A. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Grant read-only IAM permissions to any AWS principals that access the S3 bucket until the designated date.
- B. Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects.
- C. Create a new Amazon S3 bucket with S3 Versioning enabled. Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.
- D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only IAM permissions to any AWS principals that access the S3 bucket.

Answer: B

Explanation:

Question: 296

A company is running a mission-critical application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group in a single AWS Region. The application is using a database in Amazon Aurora as the data tier. A recent audit revealed that the current deployment of Aurora is not highly available.

What should a solutions architect do to improve the availability of the database?

- A. Configure an Aurora Replica.
- B. Configure storage replication.
- C. Configure storage auto scaling.
- D. Configure cross-Region replication.

Answer: B

Explanation:

Question: 297

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in every request that is sent to an Amazon API Gateway API. The solution will generate the customized images on demand. Users will receive a link that they can use to view or download their customized images. The solution must be highly available for viewing and customizing images.

What should the solutions architect do to meet these requirements MOST cost effectively?

- A. Use Amazon EC2 instances to manipulate the original images into the requested customizations. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 Instances.
- B. Use AWS Lambda to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original images into the requested customizations. Store the original images in Amazon S3. Store the manipulated images in Amazon DynamoDB. Provision an Application Load Balancer and Amazon EC2 instances to serve the content.
- D. Use Amazon EC2 instances to manipulate the original images into the requested customizations. Store the original images in Amazon S3. Store the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Answer: B

Explanation:

Question: 298

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance. What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: C

Explanation:

Question: 299

A company has a web application for travel ticketing. The application is based on a database that runs in a single data center in North America.

- a. The company wants to expand the application to serve a global user base. The company needs to deploy the application to multiple AWS Regions. Average latency must be less than 1 second on

updates to the reservation database

The company wants to have separate deployments of its web platform across multiple Regions. However, the company must maintain a single primary reservation database that is globally consistent

Which solution should a solutions architect recommend to meet these requirements?"

- A. Convert the application to use Amazon DynamoDB. Use a global table for the center reservation table. Use the correct Regional endpoint in each Regional deployment.
- B. Migrate the database to an Amazon Aurora MySQL database. Deploy Aurora Read Replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.
- C. Migrate the database to an Amazon RDS for MySQL database. Deploy MySQL read replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.
- D. Migrate the application to an Amazon Aurora Serverless database. Deploy instances of the database to each Region. Use the correct Regional endpoint in each Regional deployment to access the database. Use AWS Lambda functions to process event streams in each Region to synchronize the databases.

Answer: B

Explanation:

Question: 300

A customer is running an application on Amazon EC2 instances hosted in a private subnet of a VPC. The EC2 instances are configured in an Auto Scaling group behind an Elastic Load Balancer (ELB). The EC2 instances use a NAT gateway outbound internet access. However, the EC2 instances are not able to connect to the public internet to download software updates.

- A. The ELB is not configured with a proper health check.
- B. The route tables in the VPC are configured incorrectly.
- C. The EC2 instances are not associated with an Elastic IP address.
- D. The security group attached to the NAT gateway is configured incorrectly.
- E. The outbound rules on the security group attachment to the EC2 instances are configured incorrectly.

Answer: B, E

Explanation:

Question: 301

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

What should a solutions architect recommend to meet these requirements?

- A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions.

data with other applications

B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3 Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3

C. Stream the transactions data into Amazon Kinesis Data Streams Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB Other applications can consume the transactions data off the Kinesis data stream.

D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3 The Lambda function then stores the data in Amazon DynamoDB Other applications can consume transaction files stored in Amazon S3.

Answer: B

Explanation:

Question: 302

A company has an application that scans millions of connected devices for security threats and pushes the scan logs to an Amazon S3 bucket. A total of 70 GB of data is generated each week, and the company needs to store 3 years of data for historical reporting. The company must process aggregate, and enrich the data from Amazon S3 by performing complex analytical queries and joins in the least amount of time The aggregated dataset is visualized on an Amazon QuickSight dashboard.

What should a solutions architect recommend to meet these requirements?

A. Create and run an ETL job in AWS Glue to process the data from Amazon S3 and load it into Amazon Redshift Perform the aggregation queries on Amazon Redshift

B. Use AWS Lambda functions based on S3 PutObject event triggers to copy the incremental changes to Amazon DynamoDB Perform the aggregation queries on DynamoDB.

C. Use AWS Lambda functions based on S3 PutObject event triggers to copy the incremental changes to Amazon Aurora MySQL Perform the aggregation queries on Aurora MySQL.

D. Use AWS Glue to catalog the data in Amazon S3. Perform the aggregation queries on the cataloged tables by using Amazon Athena Query the data directly from Amazon S3

Answer: A

Explanation:

Question: 303

A company is using a VPC that is provisioned with a 10.10.1.0/24 CIDR block Because of continued growth IP address space in this block might be depleted soon. A solutions architect must add more IP address capacity to the VPC

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a new VPC Associate a larger CIDR block

B. Add a secondary CIDR block of 10 10 2 0/24 to the VPC

C. Resize the existing VPC CIDR block from 10 10 1.0/24 to 10 10.1.0

D. Establish VPC peering with a new VPC that has a CIDR block of 10.10 1.0/16

Answer: B

Explanation:

Question: 304

A company wants to automate the security assessment of its Amazon EC2 instances. The company needs to validate and demonstrate that it is meeting security and compliance standards throughout the development process.

What should a solutions architect do to meet these requirements?

- A. Use Amazon Macie to automatically discover, classify and protect the EC2 instances
- B. Use Amazon GuardDuty on the EC2 instances to publish Amazon Simple Notification Service (Amazon SNS) notifications
- C. Use Amazon Inspector with Amazon CloudWatch to publish Amazon Simple Notification Service (Amazon SNS) notifications
- D. Use Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes in the status of AWS Trusted Advisor checks

Answer: C

Explanation:

Topic 4, Exam Pool D

Question: 305

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum'?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens

Answer: A

Explanation:

Question: 306

A company's security policy requires that all AWS API activity in its AWS accounts be recorded for periodic auditing. The company needs to ensure that AWS CloudTrail is enabled on all of its current and future AWS accounts using AWS Organizations

Which solution is MOST secure?

- A. At the organization's root, define and attach a service control policy (SCP) that permits enabling CloudTrail only
- B. Create IAM groups in the organization's management account as needed Define and attach an IAM policy to the groups that prevents users from disabling CloudTrail
- C. Organize accounts into organizational units (OUs) At the organization's root define and attach a service control policy (SCP) that prevents users from disabling CloudTrail
- D. Add all existing accounts under the organization's root Define and attach a service control policy (SCP) to every account that prevents users from disabling CloudTrail

Answer: D

Explanation:

Question: 307

A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections All non-VPC traffic routes to the virtual private gateway

A development team recently created an AWS Lambda function through the console The development team needs to allow the function to access a database that runs in a private subnet in the company's data center

Which solution will meet these requirements'?

- A. Configure the Lambda function to run in the VPC with the appropriate security group
- B. Set up a VPN connection from AWS to the data center Route the traffic from the Lambda function through the VPN
- C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect
- D. Create an Elastic IP address Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface

Answer: C

Explanation:

Question: 308

A company is seeing access requests by some suspicious IP addresses The security team discovers the requests are from different IP addresses under the same CIDR range

What should a solutions architect recommend to the team?

- A. Add a rule in the inbound table of the security group to deny the traffic from that CIDR range
- B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range

- C. Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules
- D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules

Answer: C

Explanation:

Question: 309

A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata which takes less than 5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements. What should the solutions architect recommend?

- A. Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.
- B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
- C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

Answer: B

Explanation:

Question: 310

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

Answer: C

Explanation:

Question: 311

A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.

What should a solutions architect recommend?

- A. Deploy Amazon Inspector and associate it with the ALB.
- B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
- C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
- D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Answer: B

Explanation:

Question: 312

A company is hosting multiple websites for several lines of business under its registered parent domain. Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on the subdomain. The websites host static webpages, images, and server-side scripts like PHP and JavaScript.

Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.

Which combination of AWS services or features will meet these requirements? (Select TWO)

- A. AWS Batch
- B. Network Load Balancer
- C. Application Load Balancer
- D. Amazon EC2 Auto Scaling
- E. Amazon S3 website hosting

Answer: D, E

Explanation:

Question: 313

A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application. A solutions architect wants to implement a solution that is highly available, fault tolerant, and automatically scalable.

What should the solutions architect recommend?

- A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
- B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
- C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.

Zones

D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer

Answer: C

Explanation:

Question: 314

A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance. The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently. Which solution meets these requirements?

A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.

B. Store the database user credentials in AWS Systems Manager OpsCenter. Grant the necessary IAM permissions to allow the web servers to access OpsCenter.

C. Store the database user credentials in a secure Amazon S3 bucket. Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.

D.

Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.

Answer: A

Explanation:

Question: 315

A company has multiple AWS accounts with applications deployed in the us-west-2 Region. Application logs are stored within Amazon S3 buckets in each account. The company wants to build a centralized log analysis solution that uses a single S3 bucket. Logs must not leave us-west-2, and the company wants to incur minimal operational overhead.

Which solution meets these requirements and is MOST cost-effective?

A. Create an S3 Lifecycle policy that copies the objects from one of the application S3 buckets to the centralized S3 bucket.

B. Use S3 Same-Region Replication to replicate logs from the S3 buckets to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.

C. Write a script that uses the PutObject API operation every day to copy the entire contents of the buckets to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.

D. Write AWS Lambda functions in these accounts that are triggered every time logs are delivered to the S3 buckets (s3:ObjectCreated " event). Copy the logs to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.

Answer: B

Explanation:

Question: 316

A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol.

Which AWS managed service meets these requirements?

- A. Amazon EBS
- B. Amazon EC2
- C. Amazon FSx
- D. Amazon S3

Answer: C

Explanation:

Question: 317

A company is running a two-tier e-commerce website using AWS services. The current architecture uses a public-facing Elastic Load Balancer that sends traffic to Amazon EC2 instances in a private subnet. The static content is hosted on EC2 instances and the dynamic content is retrieved from a MySQL database. The application is running in the United States. The company recently started selling to users in Europe and Australia.

a. A solutions architect needs to design a solution so their international users have an improved browsing experience.

Which solution is MOST cost-effective?

- A. Host the entire website on Amazon S3.
- B. Use Amazon CloudFront and Amazon S3 to host static images.
- C. Increase the number of public load balancers and EC2 instances.
- D. Deploy the two-tier website in AWS Regions in Europe and Australia.

Answer: D

Explanation:

Question: 318

An application allows users at a company's headquarters to access product data.

a. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
- B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
- C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.

D. Create read replicas for the database Configure the read replicas with the same compute and storage resources as the source database

Answer: D

Explanation:

Question: 319

A company has a financial application that produces reports. The reports average 50 KB in size and are stored in Amazon S3. The reports are frequently accessed during the first week after production and must be stored for several years. The reports must be retrievable within 6 hours. Which solution meets these requirements MOST cost-effectively?

- A. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier after 7 days.
- B. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.
- C. Use S3 Intelligent-Tiering. Configure S3 Intelligent-Tiering to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Glacier.
- D. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier Deep Archive after 7 days.

Answer: D

Explanation:

Question: 320

A company observes an increase in Amazon EC2 costs in its most recent bill. The billing team notices unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling. How should the solutions architect generate the information with the LEAST operational overhead?

- A. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.
- B. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.
- C. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.
- D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

Answer: C

Explanation:

Question: 321

A company has a web application that includes an embedded NoSQL database. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone.

A recent increase in traffic requires the application to be highly available and for the database to be eventually consistent.

Which solution will meet these requirements with the LEAST operational overhead*?

- A. Replace the ALB with a Network Load Balancer. Maintain the embedded NoSQL database with its replication service on the EC2 instances.
- B. Replace the ALB with a Network Load Balancer. Migrate the embedded NoSQL database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS).
- C. Modify the Auto Scaling group to use EC2 instances across three Availability Zones. Maintain the embedded NoSQL database with its replication service on the EC2 instances.
- D. Modify the Auto Scaling group to use EC2 instances across three Availability Zones. Migrate the embedded NoSQL database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS).

Answer: B

Explanation:

Question: 322

A company uses Application Load Balancers (ALBs) in different AWS Regions. The ALBs receive inconsistent traffic that can spike and drop throughout the year. The company's networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.

Which solution is the MOST scalable with minimal configuration changes?

- A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions. Update the on-premises firewall's rule to allow the IP addresses of the ALBs.
- B. Migrate all ALBs in different Regions to the Network Load Balancers (NLBs). Update the on-premises firewall's rule to allow the Elastic IP addresses of all the NLBs.
- C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall's rule to allow static IP addresses associated with the accelerator.
- D. Launch a Network Load Balancer (NLB) in one Region. Register the private IP addresses of the ALBs in different Regions with the NLB. Update the on-premises firewall's rule to allow the Elastic IP address attached to the NLB.

Answer: C

Explanation:

Question: 323

A company is investigating potential solutions to collect process, and store users' service usage data. The company needs to create an analytics capability so that the company can use standard SQL queries to gather operational insights quickly. The solution must be highly available. The solution also must ensure atomicity, consistency, isolation, and durability (ACID) compliance in the data tier.

Which solution meets these requirements?

- A. Use an Amazon Timestream database.
- B. Use an Amazon Neptune database in a Multi-AZ design
- C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design
- D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS) Throughput Optimized HDD (st1) storage

Answer: C

Explanation:

Question: 324

A company runs a stateless web application in production on a group of Amazon EC2 On-Demand Instances behind an Application Load Balancer. The application experiences heavy usage during an 8-hour period each business day. Application usage is moderate and steady overnight. Application usage is low during weekends.

The company wants to minimize its EC2 costs without affecting the availability of the application. Which solution will meet these requirements?

- A. Use Spot Instances for the entire workload.
- B. Use Reserved instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs.
- C. Use On-Demand Instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs.
- D. Use Dedicated Instances for the baseline level of usage. Use On-Demand Instances for any additional capacity that the application needs.

Answer: B

Explanation:

Question: 325

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.

What should the solutions architect recommend?

- A. Implement EC2 Spot Instances
- B. Purchase EC2 Reserved Instances
- C. Implement EC2 On-Demand Instances
- D. Implement the processing on AWS Lambda

Answer: A

Explanation:

Question: 326

An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.

Which solution will meet these requirements with the LEAST amount of operational overhead?

- A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances
- B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on
- C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
- D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Answer: C

Explanation:

Question: 327

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data must be in multiple AWS Regions. How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)

Answer: C

Explanation:

Question: 328

A company is running a media store across multiple Amazon EC2 instances distributed across multiple Availability Zones in a single VPC. The company wants a high-performing solution to share data between all the EC2 instances, and prefers to keep the data within the VPC only. What should a solutions architect recommend?

- A. Create an Amazon S3 bucket and call the service APIs from each instance's application.
- B. Create an Amazon S3 bucket and configure all instances to access it as a mounted volume.
- C. Configure an Amazon Elastic Block Store (Amazon EBS) volume and mount it across all instances.
- D. Configure an Amazon Elastic File System (Amazon EFS) file system and mount it across all instances.

instances

Answer: C

Explanation:

Question: 329

A solutions architect is planning the deployment of a new static website. The solution must minimize costs and provide at least 99% availability. Which solution meets these requirements?

- A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.
- B. Deploy the application to Amazon EC2 instances that run in two AWS Regions and two Availability Zones.
- C. Deploy the application to an Amazon S3 bucket that has versioning and cross-Region replication enabled.
- D. Deploy the application to an Amazon EC2 instance that runs in one AWS Region and one Availability Zone.

Answer: A

Explanation:

Question: 330

A development team stores its Amazon RDS MySQL DB instance user name and password credentials in a configuration file. The configuration file is stored as plaintext on the root device volume of the team's Amazon EC2 instance. When the team's application needs to reach the database, it reads the file and loads the credentials into the code. The team has modified the permissions of the configuration file so that only the application can read its content. A solutions architect must design a more secure solution. What should the solutions architect do to meet this requirement?

- A. Store the configuration file in Amazon S3. Grant the application access to read the configuration file.
- B. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.
- C. Enable SSL connections on the database instance. Alter the database user to require SSL when logging in.
- D. Move the configuration file to an EC2 instance store, and create an Amazon Machine Image (AMI) of the instance. Launch new instances from this AMI.

Answer: D

Explanation:

Question: 331

A solution architect is designing an application for a two-step order across. The first step is

synchronous and must return to the user with little latency. The second step takes longer so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received.

How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues
- B. Use an AWS Lambda function along with Amazon SQS standard queues.
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
- D. Create an SNS topic subscribe an Amazon SQS Standard queue to that topic.

Answer: C

Explanation:

Question: 332

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time. Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Answer: A

Explanation:

Question: 333

A company is running a database on Amazon Aurora. The database is idle every evening. An application that performs extensive reads on the database experiences performance issues during morning hours when user traffic spikes. During these peak periods, the application receives timeout errors when reading from the database. The company does not have a dedicated operations team and needs an automated solution to address the performance issues. Which actions should a solutions architect take to automatically adjust to the increased read load on the database? (Select TWO)

- A. Migrate the database to Aurora Serverless
- B. Increase the instance size of the Aurora database
- C. Configure Aurora Auto Scaling with Aurora Replicas.
- D. Migrate the database to an Aurora multi-master cluster

E. Migrate the database to an Amazon RDS for MySQL Multi-AZ deployment

Answer: A, C

Explanation:

Question: 334

An ecommerce company uses an Amazon Aurora DB cluster to store customer transactions. The company also maintains a separate Amazon DynamoDB table that contains item sales information. The company wants the DB cluster to invoke a recently deployed AWS Lambda function to update the DynamoDB table every time a row is inserted into the database.

Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

- A. Modify the Lambda function to allow outbound communication to the DB cluster
- B. Modify the DB cluster to allow outbound communication to the Lambda function.
- C. Modify the DB cluster to allow outbound communication to the DynamoDB table
- D. Ensure that the DB cluster has an IAM role that allows the DB cluster to invoke Lambda functions.
- E. Ensure that the Lambda function has an IAM role that allows Lambda to invoke functions on the DB cluster

Answer: C, E

Explanation:

Question: 335

A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL.

What should a solutions architect do to meet these requirements?

- A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
- B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.
- C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
- D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Answer: D

Explanation:

Question: 336

A company is planning to build a new web application on AWS. The company expects predictable traffic most of the year and very high traffic on occasion. The web application needs to be highly

available and fault tolerant with minimal latency.

What should a solutions architect recommend to meet these requirements?

- A. Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions each with one Amazon EC2 instance
- B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones
- C. Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones
- D. Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group

Answer: B

Explanation:

Question: 337

A company has a hybrid application hosted on multiple on-premises servers with static IP addresses. There is already a VPN that provides connectivity between the VPC and the on-premises network. The company wants to distribute TCP traffic across the on-premises servers for internet users. What should a solutions architect recommend to provide a highly available and scalable solution?

- A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB
- B. Launch an internet-facing Application Load Balancer (ALB) and register on-premises IP addresses with the ALB
- C. Launch an Amazon EC2 instance, attach an Elastic IP address, and distribute traffic to the on-premises servers
- D. Launch an Amazon EC2 instance with public IP addresses in an Auto Scaling group and distribute traffic to the on-premises servers

Answer: B

Explanation:

Question: 338

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated. Which solution achieves these goals MOST efficiently?

- A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.
- B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.
- C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send

data to the audit system when instances are launched and terminated

D. Run a custom script on the instance operating system to send data to the audit system Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated

Answer: B

Explanation:

Question: 339

A company offers a food delivery service that is growing rapidly Because of the growth the company's order processing system is experiencing scaling problems during peak traffic hours. The current architecture includes the following;

- A group of Amazon EC2 instances that run in an Amazon EC2 Auto Scaling group to collect orders from the application
 - Another group of EC2 instances that run in an Amazon EC2 Auto Scaling group to fulfill orders
- The order collection process occurs quickly, but the order fulfillment process can take longer Data must not be lost because of a scaling event

A solutions architect must ensure that the order collection process and the order fulfillment process can both scale properly during peak traffic hours The solution must optimize utilization of the company's AWS resources

Which solution meets these requirements'?

- A. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure each Auto Scaling group's minimum capacity according to peak workload values
- B. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic that creates additional Auto Scaling groups on demand
- C. Provision two Amazon Simple Queue Service (Amazon SQS) queues one for order collection and another for order fulfillment Configure the EC2 instances to poll their respective queue Scale the Auto Scaling groups based on notifications that the queues send
- D. Provision two Amazon Simple Queue Service (Amazon SQS) queues one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation Scale the Auto Scaling groups based on this metric.

Answer: D

Explanation:

Question: 340

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modelling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.

The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution

should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files

Which combination of AWS services meets these requirements?

- A. Amazon FSx for Lustre integrated with Amazon S3
- B. Amazon FSx for Windows File Server integrated with Amazon S3
- C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
- D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD(gp2) volume

Answer: A

Explanation:

Question: 341

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

- A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
- D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

Answer: A

Explanation:

Question: 342

A company wants to use a custom distributed application that calculates various profit and loss scenarios. To achieve this goal, the company needs to provide a network connection between its Amazon EC2 instances. The connection must minimize latency and must maximize throughput.

Which solution will meet these requirements?

- A. Provision the application to use EC2 Dedicated Hosts of the same instance type.
- B. Configure a placement group for EC2 instances that have the same instance type
- C. Use multiple AWS elastic network interfaces and link aggregation
- D. Configure AWS PrivateLink for the EC2 instances

Answer: A

Explanation:

Question: 343

A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS, and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times. Which action will be MOST effective in accomplishing this?

- A. Replace the SQS queue with Amazon Kinesis Data Firehose
- B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier
- C. Add an Amazon CloudFront distribution to cache the responses for the web tier.
- D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth

Answer: C

Explanation:

Question: 344

A company recently migrated a legacy application from an on-premises data center to AWS. The application is running on an Amazon EC2 instance. The EC2 instance is deployed in a private subnet in a VPC without inbound internet access. The application support team requires SSH access to the operating system to perform periodic maintenance. Which solution provides secure access with the LEAST operational effort?

- A. Configure AWS Client VPN to access the VPC. Update the EC2 instance security group inbound rules to allow access from Client VPN.
- B. Configure AWS Site-to-Site VPN to access the VPC. Update the EC2 instance security group inbound rules to allow access from Site-to-Site VPN.
- C. Attach the AmazonSSMManagedInstanceCore IAM policy to the EC2 instance role. Use AWS Systems Manager Session Manager to enable SSH connection.
- D. Deploy a bastion host in a public subnet. Allow SSH access to the bastion host from the internet. Update the EC2 instance security group inbound rules to allow access from the bastion host.

Answer: D

Explanation:

Question: 345

An application development team is designing a microservice that will convert large images to smaller compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket. A solutions architect needs to design a solution that uses durable stateless components to process the images automatically.

Which combination of actions will meet these requirements? (Select TWO)

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
- B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.
- C. Configure the Lambda function to monitor the S3 bucket for new uploads. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.
- D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.
- E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket. When an image is uploaded, send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing.

Answer: A, B

Explanation:

Question: 346

A solutions architect creates a VPC that includes two public subnets and two private subnets. A corporate security mandate requires the solutions architect to launch all Amazon EC2 instances in a private subnet. However, when the solutions architect launches an EC2 instance that runs a web server on ports 80 and 443 in a private subnet, no external internet traffic can connect to the server. What should the solutions architect do to resolve this issue?

- A. Attach the EC2 instance to an Auto Scaling group in a private subnet. Ensure that the DNS record for the website resolves to the Auto Scaling group identifier.
- B. Provision an internet-facing Application Load Balancer (ALB) in a public subnet. Add the EC2 instance to the target group that is associated with the ALB. Ensure that the DNS record for the website resolves to the ALB.
- C. Launch a NAT gateway in a private subnet. Update the route table for the private subnets to add a default route to the NAT gateway. Attach a public Elastic IP address to the NAT gateway.
- D. Ensure that the security group that is attached to the EC2 instance allows HTTP traffic on port 80 and HTTPS traffic on port 443. Ensure that the DNS record for the website resolves to the public IP address of the EC2 instance.

Answer: A

Explanation:

Question: 347

A company is preparing to deploy a data lake on AWS. A solutions architect must define the encryption strategy for data at rest in Amazon S3. The company's security policy states

- Keys must be rotated every 90 days
- Strict separation of duties between key users and key administrators must be implemented
- Auditing key usage must be possible

What should the solutions architect recommend?

- A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs)
- B. Server-side encryption with AWS KMS managed keys (SSE-KMS) with AWS managed customer master keys (CMKs)
- C. Server-side encryption with Amazon S3 managed keys (SSE-S3) with customer managed customer master keys (CMKs)
- D. Server-side encryption with Amazon S3 managed keys (SSE-S3) with AWS managed customer master keys (CMKs)

Answer: B

Explanation:

Question: 348

The financial application at a company stores monthly reports in an Amazon S3 bucket. The vice president of finance has mandated that all access to these reports be logged and that any modifications to the log files be detected.

Which actions can a solutions architect take to meet these requirements?

- A. Use S3 server access logging on the bucket that houses the reports with the read and write data events and log file validation options enabled
- B. Use S3 server access logging on the bucket that houses the reports with the read and write management events and log file validation options enabled
- C. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write data events on the S3 bucket that houses the reports. Log these events to a new bucket and enable log file validation.
- D. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.

Answer: C

Explanation:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html>

Question: 349

A solution architect has created two IAM policies. Policy1 and Policy2 . Both policies are attached to an IAM group.

```
Policy1
{
  "Version": "2012-10-17", "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:Get*",
        "iam:List*",
        "kms:List*",
        "ec2:*",
        "ds:*",
        "logs:Get*",
        "logs:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

```
Policy2
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ds:Delete*",
      "Resource": "*"
    }
  ]
}
```

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

- A. Deleting IAM users
- B. Deleting directories
- C. Deleting Amazon EC2 instances
- D. Deleting logs from Amazon CloudWatch Logs

Answer: C

Explanation:

Question: 350

A company runs a public three-Tier web application in a VPC The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet The company needs a managed solution that minimizes operational maintenance

Which solution meets these requirements"

- A. Provision a NAT instance in a public subnet Modify each private subnets route table with a default route that points to the NAT instance
- B. Provision a NAT instance in a private subnet Modify each private subnet's route table with a

default route that points to the NAT instance

C. Provision a NAT gateway in a public subnet Modify each private subnet's route table with a default route that points to the NAT gateway

D. Provision a NAT gateway in a private subnet Modify each private subnet's route table with a default route that points to the NAT gateway

Answer: C

Explanation:

Question: 351

A company hosts a marketing website in an on-premises data center. The website consists of static documents and runs on a single server. An administrator updates the website content infrequently and uses an SFTP client to upload new documents.

The company decides to host its website on AWS and to use Amazon CloudFront. The company's solutions architect creates a CloudFront distribution. The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin. Which solution will meet these requirements?

A. Create a virtual server by using Amazon Lightsail. Configure the web server in the Lightsail instance. Upload website content by using an SFTP client.

B. Create an AWS Auto Scaling group for Amazon EC2 instances. Use an Application Load Balancer. Upload website content by using an SFTP client.

C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI). Upload website content by using the AWS CLI.

D. Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client.

Answer: C

Explanation:

Question: 352

A pharmaceutical company is developing a new drug. The volume of data that the company generates has grown exponentially over the past few months. The company's researchers regularly require a subset of the entire dataset to be immediately available with minimal lag. However, the entire dataset does not need to be accessed on a daily basis. All the data currently resides in on-premises storage arrays, and the company wants to reduce ongoing capital expenses.

Which storage solution should a solutions architect recommend to meet these requirements?

A. Run AWS DataSync as a scheduled cron job to migrate the data to an Amazon S3 bucket on an ongoing basis.

B. Deploy an AWS Storage Gateway file gateway with an Amazon S3 bucket as the target storage. Migrate the data to the Storage Gateway appliance.

C. Deploy an AWS Storage Gateway volume gateway with cached volumes with an Amazon S3 bucket as the target storage. Migrate the data to the Storage Gateway appliance.

D. Configure an AWS Site-to-Site VPN connection from the on-premises environment to AWS.

Migrate data to an Amazon Elastic File System (Amazon EFS) file system.

Answer: C

Explanation:

Question: 353

A company has deployed a database in Amazon RDS for MySQL. Due to increased transactions, the database support team is reporting slow reads against the DB instance and recommends adding a read replica.

Which combination of actions should a solutions architect take before implementing this change? (Select TWO.)

- A. Enable binlog replication on the RDS primary node.
- B. Choose a failover priority for the source DB instance.
- C. Allow long-running transactions to complete on the source DB instance.
- D. Create a global table and specify the AWS Regions where the table will be available.
- E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0.

Answer: B, E

Explanation:

Question: 354

A solutions architect is designing a shared storage solution for a web application that is deployed across multiple Availability Zones. The web application runs on Amazon EC2 instances that are in an Auto Scaling group. The company plans to make frequent changes to the content. The solution must have strong consistency in returning the new content as soon as the changes occur.

Which solutions meet these requirements? (Select TWO.)

- A. Use AWS Storage Gateway Volume Gateway Internet Small Computer Systems Interface (iSCSI) block storage that is mounted to the individual EC2 instances.
- B. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on the individual EC2 instances.
- C. Create a shared Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the individual EC2 instances.
- D. Use AWS DataSync to perform continuous synchronization of data between EC2 hosts in the Auto Scaling group.
- E. Create an Amazon S3 bucket to store the web content. Set the metadata for the Cache-Control header to no-cache. Use Amazon CloudFront to deliver the content.

Answer: B, C

Explanation:

Question: 355

A company manages and runs a critical data management application in containers that are hosted on Amazon Elastic Container Service (Amazon ECS). The application has endpoints that are exposed through Application Load Balancers (ALBs). The application uses an Amazon Elastic File System (Amazon EFS) file system mount for persistent data storage. The company has configured Amazon ECS to use a minimal IAM instance role.

Which combination of actions should a solutions architect take to improve the overall security posture of the application? (Select TWO.)

- A. Decompose the Amazon ECS IAM instance role. Use only ECS task roles.
- B. Enable EFS encryption in transit to protect data that is being written to Amazon EFS.
- C. Use AWS Config to define patch management policies on the container instances.
- D. Use Amazon Macie integration with Amazon EFS to monitor and protect sensitive information in the file system.
- E. Use Amazon GuardDuty to authenticate data access between the ALBs and the container instances.

Answer: C, D

Explanation:

Question: 356

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda

a. Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of "application" and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.

Which solution meets these requirements?

- A. Use AWS CloudTrail to generate a list of resources with the application tag.
- B. Use the AWS CLI to query each service across all Regions to report the tagged components.
- C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.
- D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

Answer: D

Explanation:

Question: 357

A company runs a static website through its on-premises data center. The company has multiple servers that handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable. The company wants to expand its presence globally and plans to triple its website traffic.

What should a solutions architect recommend to meet these requirements?

- A. Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.
- B. Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.
- C. Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.
- D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

Answer: D

Explanation:

Question: 358

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Answer: B

Explanation:

Question: 359

A solution architect has configured the following IAM policy.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "lambda:CreateFunction",
        "lambda:DeleteFunction"
      ],
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "220.100.16.0/20"
        }
      }
    }
  ]
}

```

Which action will be allowed by the policy?

Which action will be allowed by the policy?

- A. An AWS Lambda function can be deleted from any network.
- B. An AWS Lambda function can be created from any network.
- C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.
- D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network

Answer: C

Explanation:

Question: 360

A company wants to improve the availability and performance of its hybrid application. The application consists of a stateful TCP-based workload hosted on Amazon EC2 instances in different AWS Regions and a stateless UDP-based workload hosted on premises.

Which combination of actions should a solutions architect take to improve availability and performance? (Select TWO.)

- A. Create an accelerator using AWS Global Accelerator. Add the load balancers as endpoints.
- B. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the load balancers.
- C. Configure two Application Load Balancers in each Region. The first will route to the EC2 endpoints, and the second will route to the on-premises endpoints.
- D. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure a Network Load Balancer in each Region that routes to the on-premises endpoints.

E. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure an Application Load Balancer in each Region that routes to the on-premises endpoints.

Answer: A, B

Explanation:

Question: 361

A solutions architect needs to host a high performance computing (HPC) workload in the AWS Cloud. The workload will run on hundreds of Amazon EC2 instances and will require parallel access to a shared file system to enable distributed processing of large datasets. Datasets will be accessed across multiple instances simultaneously. The workload requires access latency within 1 ms. After processing has completed, engineers will need access to the dataset for manual postprocessing. Which solution will meet these requirements?

- A. Use Amazon Elastic File System (Amazon EFS) as a shared file system. Access the dataset from Amazon EFS.
- B. Mount an Amazon S3 bucket to serve as the shared file system. Perform postprocessing directly from the S3 bucket.
- C. Use Amazon FSx for Lustre as a shared file system. Link the file system to an Amazon S3 bucket for postprocessing.
- D. Configure AWS Resource Access Manager to share an Amazon S3 bucket so that it can be mounted to all instances for processing and postprocessing.

Answer: C

Explanation:

Question: 362

A company is upgrading its critical web-based application. The application is hosted on Amazon EC2 instances that are part of an Auto Scaling group behind an Application Load Balancer (ALB). The company wants to test the new configurations with a specific amount of traffic before the company begins to route all traffic to the upgraded application. How should a solutions architect design the architecture to meet these requirements?

- A. Create a new launch template. Associate the new launch template with the Auto Scaling group. Attach the Auto Scaling group to the ALB. Distribute traffic by using redirect rules.
- B. Create a new launch template. Create an additional Auto Scaling group. Associate the new launch template with the additional Auto Scaling group. Attach the additional Auto Scaling group to the ALB. Distribute traffic by using weighted target groups.
- C. Create a new launch template. Create an additional Auto Scaling group. Associate the new launch template with the additional Auto Scaling group. Create an additional ALB. Attach the additional Auto Scaling group to the additional ALB. Use an Amazon Route 53 failover routing policy to route traffic.
- D. Create a new launch template. Create an additional Auto Scaling group. Associate the new launch template with the additional Auto Scaling group. Create an additional ALB. Attach the additional Auto Scaling group to the additional ALB. Use an Amazon Route 53 weighted routing policy to route

traffic.

Answer: A

Explanation:

Question: 363

A trucking company is deploying an application that will track the GPS coordinates of all the company's trucks. The company needs a solution that will generate real-time statistics based on metadata lookups with high read throughput and microsecond latency. The database must be fault tolerant and must minimize operational overhead and development effort.

Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

- A. Use Amazon DynamoDB as the database.
- B. Use Amazon Aurora MySQL as the database.
- C. Use Amazon RDS for MySQL as the database.
- D. Use Amazon ElastiCache as the caching layer.
- E. Use Amazon DynamoDB Accelerator (DAX) as the caching layer.

Answer: A, E

Explanation:

Question: 364

A company is planning to run a group of Amazon EC2 instances that connect to an Amazon Aurora database. The company has built an AWS CloudFormation template to deploy the EC2 instances and the Aurora DB cluster. The company wants to allow the instances to authenticate to the database in a secure way. The company does not want to maintain static database credentials.

Which solution meets these requirements with the LEAST operational effort?

- A. Create a database user with a user name and password. Add parameters for the database user name and password to the CloudFormation template. Pass the parameters to the EC2 instances when the instances are launched.
- B. Create a database user with a user name and password. Store the user name and password in AWS Systems Manager Parameter Store. Configure the EC2 instances to retrieve the database credentials from Parameter Store.
- C. Configure the DB cluster to use IAM database authentication. Create a database user to use with IAM authentication. Associate a role with the EC2 instances to allow applications on the instances to access the database.
- D. Configure the DB cluster to use IAM database authentication with an IAM user. Create a database user that has a name that matches the IAM user. Associate the IAM user with the EC2 instances to allow applications on the instances to access the database.

Answer: C

Explanation:

Question: 365

A development team is creating an event-based application that uses AWS Lambda functions. Events will be generated when files are added to an Amazon S3 bucket. The development team currently has Amazon Simple Notification Service (Amazon SNS) configured as the event target from Amazon S3.

What should a solutions architect do to process the events from Amazon S3 in a scalable way?

A. Create an SNS subscription that processes the event in Amazon Elastic Container Service (Amazon ECS) before the event runs in Lambda.

B. Create an SNS subscription that processes the event in Amazon Elastic Kubernetes Service (Amazon EKS) before the event runs in Lambda.

C. Create an SNS subscription that sends the event to Amazon Simple Queue Service (Amazon SQS). Configure the SQS queue to trigger a Lambda function.

D. Create an SNS subscription that sends the event to AWS Server Migration Service (AWS SMS). Configure the Lambda function to poll from the SMS event.

Answer: D

Explanation:

Question: 366

A company is running a multi-tier ecommerce web application in the AWS Cloud. The web application is running on Amazon EC2 instances. The database tier is on a provisioned Amazon Aurora MySQL DB cluster with a writer and a reader in a Multi-AZ environment. The new requirement for the database tier is to serve the application to achieve continuous write availability through an instance failover.

What should a solutions architect do to meet this new requirement?

A. Add a new AWS Region to the DB cluster for multiple writes.

B. Add a new reader in the same Availability Zone as the writer.

C. Migrate the database tier to an Aurora multi-master cluster.

D. Migrate the database tier to an Aurora DB cluster with parallel query enabled.

Answer: C

Explanation:

Question: 367

A company is building a document storage application on AWS. The application runs on Amazon EC2 instances in multiple Availability Zones. The company requires the document store to be highly available. The documents need to be returned immediately when requested. The lead engineer has configured the application to use Amazon Elastic Block Store (Amazon EBS) to store the documents, but is willing to consider other options to meet the availability requirement.

What should a solutions architect recommend?

A. Snapshot the EBS volumes regularly and build new volumes using those snapshots in additional Availability Zones.

B. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3.

- C. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3 Glacier.
- D. Use at least three Provisioned IOPS EBS volumes for EC2 instances Mount the volumes to the EC2 instances in a RAID 5 configuration.

Answer: B

Explanation:

Question: 368

A solutions architect needs to design a system to store client case files. The files are core company assets and are important. The number of files will grow over time. The files must be simultaneously accessible from multiple application servers that run on Amazon EC2 instances. The solution must have built-in redundancy. Which solution meets these requirements?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon S3 Glacier Deep Archive
- D. AWS Backup

Answer: A

Explanation:

Question: 369

A company runs an online ticketing application with backend services that run on Amazon EC2 instances. The EC2 instances belong to an Auto Scaling group and run behind an Application Load Balancer. The application experiences periods of high user traffic when a popular event is posted online. The company wants a solution that will be able to handle increases in user traffic without affecting the user experience.

What should a solutions architect do to meet these requirements?

- A. Configure a scheduled scaling policy for peak hours with a recurrence schedule set to every day.
- B. Configure a target tracking scaling policy that uses the average aggregate CPU utilization target metric.
- C. Configure a step scaling policy that is based on an Amazon CloudWatch alarm that monitors CPU utilization.
- D. Configure an Application Load Balancer health check that increases the Auto Scaling group capacity whenever the application returns HTTP 503 error codes.

Answer: B

Explanation:

Question: 370

A company is running a photo hosting service in the us-east-1 Region. The service enables users

across multiple countries to upload and view photos. Some photos are heavily viewed for months, and others are viewed for less than a week. The application allows uploads of up to 20 MB for each photo. The service uses the photo metadata to determine which photos to display to each user. Which solution provides the appropriate user access MOST cost-effectively?

- A. Store the photos in Amazon DynamoDB. Turn on DynamoDB Accelerator (DAX) to cache frequently viewed items.
- B. Store the photos in the Amazon S3 Intelligent-Tiering storage class. Store the photo metadata and its S3 location in DynamoDB.
- C. Store the photos in the Amazon S3 Standard storage class. Set up an S3 Lifecycle policy to move photos older than 30 days to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Use the object tags to keep track of metadata.
- D. Store the photos in the Amazon S3 Glacier storage class. Set up an S3 Lifecycle policy to move photos older than 30 days to the S3 Glacier Deep Archive storage class. Store the photo metadata and its S3 location in Amazon Elasticsearch Service (Amazon ES).

Answer: A

Explanation:

Question: 371

A company has no existing file share services. A new project requires access to file storage that is mountable as a drive for on-premises desktops. The file server must authenticate users to an Active Directory domain before they are able to access the storage.

Which service will allow Active Directory users to mount storage as a drive on their desktops?

- A. Amazon S3 Glacier
- B. AWS DataSync
- C. AWS Snowball Edge
- D. AWS Storage Gateway

Answer: D

Explanation:

Question: 372

A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour.

What should the solutions architect recommend to meet these requirements?

- A. Configure DynamoDB global tables. For RPO recovery, point the application to a different AWS Region.
- B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.
- C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.

D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

Answer: D

Explanation:

Question: 373

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. The company must not make any changes to the application. What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 Standard bucket with access to the web servers.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.
- D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Answer: C

Explanation:

Question: 374

A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company's operations team needs to be notified when RDP or SSH access to an environment has been established. What should a solutions architect recommend to meet these requirements?

- A. Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.
- B. Configure the EC2 instances with an IAM instance profile that has an IAM role with the AmazonSSMManagedInstanceCore policy attached.
- C. Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state.
- D. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

Answer: D

Explanation:

Question: 375

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be

encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

- A. Server-Side Encryption with keys stored in an S3 bucket
- B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
- C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Answer: D

Explanation:

Question: 376

A company is planning to move a dynamic web application to AWS. Application assets are stored in a Linux file server. The total volume of data is 140 TB, and the company has 100 Mbps of internet bandwidth available. The company does not want to make any changes to the application during migration. File permissions must be preserved.

How should a solutions architect migrate and store the data to meet these requirements?

- A. Transfer the data by using the file interface for AWS Snowball. Use Amazon Elastic File System (Amazon EFS) as the migration destination and for storage.
- B. Transfer the data by using the Amazon S3 interface for AWS Snowball. Use Amazon FSx for Lustre as the migration destination and for storage.
- C. Transfer the data by using the AWS CLI `s3 cp` command. Use Amazon EC2 with Amazon Elastic Block Store (Amazon EBS) as the migration destination and for storage.
- D. Transfer the data by using AWS DataSync. Use AWS Storage Gateway File Gateway as the migration destination and for storage.

Answer: A

Explanation:

Question: 377

A company wants its public web application to run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The application must use a publicly trusted SSL certificate.

Which solution will meet these requirements MOST cost-effectively?

- A. Provision a public SSL/TLS certificate through AWS Certificate Manager (ACM). Configure the new certificate on the HTTPS listener for the ALB.
- B. Use AWS Certificate Manager Private Certificate Authority to issue an SSL/TLS certificate. Configure the new certificate on the HTTPS listener for the ALB.
- C. Create a self-signed certificate on one of the EC2 instances in the Auto Scaling group. Export the certificate, and configure it on the HTTPS listener for the ALB.
- D. Deploy an EC2-hosted certificate authority (CA). Import a trusted root certificate. Issue a new

SSL/TLS certificate. Configure the new certificate on the HTTPS listener for the ALB.

Answer: A

Explanation:

Question: 378

A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime.

What should a solutions architect do to meet these requirements with the LEAST amount of downtime?

- A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be launched when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be launched when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

Answer: A

Explanation:

Question: 379

A company wants to monitor its AWS costs for financial review. The cloud operations team is designing an architecture in the AWS Organizations management account to query AWS Cost and Usage Reports for all member accounts. The team must run this query once a month and provide a detailed analysis of the bill.

Which solution is the MOST scalable and cost-effective way to meet these requirements?

- A. Enable Cost and Usage Reports in the management account. Deliver reports to Amazon Kinesis. Use Amazon EMR for analysis.
- B. Enable Cost and Usage Reports in the management account. Deliver the reports to Amazon S3. Use Amazon Athena for analysis.
- C. Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon S3. Use Amazon Redshift for analysis.
- D. Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon Kinesis. Use Amazon QuickSight for analysis.

Answer: B

Explanation:

Question: 380

A solutions architect is creating an application. The application will run on Amazon EC2 instances in private subnets across multiple Availability Zones in a VPC. The EC2 instances will frequently access large files that contain confidential information. These files are stored in Amazon S3 buckets for processing. The solutions architect must optimize the network architecture to minimize data transfer costs.

What should the solutions architect do to meet these requirements?

- A. Create a gateway endpoint for Amazon S3 in the VPC. In the route tables for the private subnets, add an entry for the gateway endpoint.
- B. Create a single NAT gateway in a public subnet. In the route tables for the private subnets, add a default route that points to the NAT gateway.
- C. Create an AWS PrivateLink interface endpoint for Amazon S3 in the VPC. In the route tables for the private subnets, add an entry for the interface endpoint.
- D. Create one NAT gateway for each Availability Zone in public subnets. In each of the route tables for the private subnets, add a default route that points to the NAT gateway in the same Availability Zone.

Answer: D

Explanation:

Question: 381

A company needs to build a reporting solution on AWS. The solution must support SQL queries that data analysts run on the data.

- a. The data analysts will run lower than 10 total queries each day. The company generates 3 GB of new data daily in an on-premises relational database. This data needs to be transferred to AWS to perform reporting tasks.

What should a solutions architect recommend to meet these requirements at the LOWEST cost?

- A. Use AWS Database Migration Service (AWS DMS) to replicate the data from the on-premises database into Amazon S3. Use Amazon Athena to query the data.
- B. Use an Amazon Kinesis Data Firehose delivery stream to deliver the data into an Amazon Elasticsearch Service (Amazon ES) cluster. Run the queries in Amazon ES.
- C. Export a daily copy of the data from the on-premises database. Use an AWS Storage Gateway file gateway to store and copy the export into Amazon S3. Use an Amazon EMR cluster to query the data.
- D. Use AWS Database Migration Service (AWS DMS) to replicate the data from the on-premises database and load it into an Amazon Redshift cluster. Use the Amazon Redshift cluster to query the data.

Answer: A

Explanation:

Question: 382

A company wants to use AWS Systems Manager to manage a fleet of Amazon EC2 instances. According to the company's security requirements, no EC2 instances can have internet access. A solutions architect needs to design network connectivity from the EC2 instances to Systems Manager while fulfilling this security obligation.

Which solution will meet these requirements?

- A. Deploy the EC2 instances into a private subnet with no route to the internet.
- B. Configure an interface VPC endpoint for Systems Manager. Update routes to use the endpoint.
- C. Deploy a NAT gateway into a public subnet. Configure private subnets with a default route to the NAT gateway.
- D. Deploy an internet gateway. Configure a network ACL to deny traffic to all destinations except Systems Manager.

Answer: C

Explanation:

Question: 383

A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deployed on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. The company needs the ability to shift traffic from resources in one region to another.

What should a solutions architect recommend?

- A. Configure an Amazon Route 53 latency routing policy.
- B. Configure an Amazon Route 53 geolocation routing policy.
- C. Configure an Amazon Route 53 geoproximity routing policy.
- D. Configure an Amazon Route 53 multivalue answer routing policy.

Answer: C

Explanation:

Geoproximity routing policy – Use when you want to route traffic based on the location of your resources and, optionally, "shift traffic from resources in one location to resources in another". Using "Bias" you can expand or shrink size of the geographic region and shift traffic from one geographic region to another. To optionally change the size of the geographic region from which Route 53 routes traffic to a resource, specify the applicable value for the bias: To expand the size of the geographic region from which Route 53 routes traffic to a resource, specify a positive integer from 1 to 99 for the bias. Route 53 shrinks the size of adjacent regions. To shrink the size of the geographic region from which Route 53 routes traffic to a resource, specify a negative bias of -1 to -99. Route 53 expands the size of adjacent regions. <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

Question: 384

A company needs to store data from its healthcare application. The application's data frequently

changes. A new regulation requires audit access at all levels of the stored data. The company hosts the application on an on-premises infrastructure that is running out of storage capacity. A solutions architect must securely migrate the existing data to AWS while satisfying the new regulation.

Which solution will meet these requirements?

- A. Use AWS DataSync to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
- B. Use AWS Snowcone to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.
- C. Use Amazon S3 Transfer Acceleration to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
- D. Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

Answer: A

Explanation:

Question: 385

A company has two AWS accounts: Production and Development. The company needs to push code changes in the Development account to the Production account. In the alpha phase, only two developers on the development team need access to the Production account. In the beta phase, more developers will need access to perform testing.

Which solution will meet these requirements?

- A. Create two policy documents by using the AWS Management Console in each account. Assign the policy to developers who need access.
- B. Create an IAM role in the Development account. Grant the IAM role access to the Production account. Allow developers to assume the role.
- C. Create an IAM role in the Production account. Define a trust policy that specifies the Development account. Allow developers to assume the role.
- D. Create an IAM group in the Production account. Add the group as a principal in a trust policy that specifies the Production account. Add developers to the group.

Answer: C

Explanation:

Question: 386

A large international university has deployed all of its compute services in the AWS Cloud. These services include Amazon EC2, Amazon RDS, and Amazon DynamoDB. The university currently relies on many custom scripts to backup its infrastructure. However, the university wants to centralize management and automate data backups as much as possible by using AWS native options.

Which solution will meet these requirements?

- A. Use third-party backup software with an AWS Storage Gateway tape gateway virtual tape library.
- B. Use AWS Backup to configure and monitor all backups for the services in use.
- C. Use AWS Config to set lifecycle management to take snapshots of all data sources on a schedule.
- D. Use AWS Systems Manager State Manager to manage the configuration and monitoring of backup tasks.

Answer: B

Explanation:

Question: 387

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only. What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 Intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

Explanation:

Question: 388

A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website.

Which solution meets these requirements MOST cost-effectively?

- A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.
- B. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.
- C. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.
- D. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

Answer: C

Explanation:

Question: 389

A company built an application with Docker containers and needs to run the application in the AWS Cloud. The company wants to use a managed service to host the application.

The solution must scale in and out appropriately according to demand on the individual container

services. The solution also must not result in additional operational overhead or infrastructure to manage. Which solutions will meet these requirements? (Select TWO.)

- A. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
- B. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate.
- C. Provision an Amazon API Gateway API. Connect the API to AWS Lambda to run the containers.
- D. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes.
- E. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes.

Answer: A,B

Explanation:

Question: 390

A company must save all the email messages that its employees send to customers for a period of 12 months. The messages are stored in a binary format and vary in size from 1 KB to 20 KB. The company has selected Amazon S3 as the storage service for the messages. Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)

- A. Create an S3 bucket policy that denies the s3 Delete Object action.
- B. Create an S3 lifecycle configuration that deletes the messages after 12 months.
- C. Upload the messages to Amazon S3. Use S3 Object Lock in governance mode.
- D. Upload the messages to Amazon S3. Use S3 Object Lock in compliance mode.
- E. Use S3 Inventory. Create an AWS Batch job that periodically scans the inventory and deletes the messages after 12 months.

Answer: B,D

Explanation:

Question: 391

A company is building its web application by using containers on AWS. The company requires three instances of the web application to run at all times. The application must be highly available and must be able to scale to meet increases in demand. Which solution meets these requirements?

- A. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks.
- B. Use the Amazon EC2 launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
- C. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in three different Availability Zones. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks.

D. Use the Amazon EC2 launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has one container instance in two different Availability Zones. Create definition for the web application. Place two tasks on one container instance. Place one task on the remaining container instance.

Answer: C

Explanation:

Question: 392

A company runs a fleet of web services using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases. Which solution meets these requirements?

- A. Enable a Multi-AZ deployment for the DB instance.
- B. Enable auto scaling for the DB instance in one Availability Zone.
- C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
- D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Answer: A

Explanation:

Question: 393

A company recently migrated multiple applications and databases from an on-premises data center to the AWS Cloud. Most of the applications run on AWS Fargate, and some of the applications run on Amazon EC2 instances. Most of the databases run on Amazon RDS, and a small number of databases run on EC2 instances.

All the applications and databases must be available 24 hours a day, 7 days a week. The company uses AWS Organizations to manage AWS accounts. A solutions architect must recommend how to minimize the cost of these workloads over the next 3 years.

Which solution meets these requirements?

- A. Purchase All Upfront Reserved Instances with a 3-year term for Amazon EC2 and Fargate.
- B. Purchase All Upfront Reserved Instances with a 3-year term for Amazon EC2 and Amazon RDS.
- C. Purchase All Upfront Compute Savings Plans with a 3-year term for Amazon EC2 and Fargate. Purchase All Upfront Reserved Instances with a 3-year term for Amazon RDS.
- D. Purchase All Upfront EC2 Instance Savings Plans with a 3-year term for Amazon EC2 and Fargate. Purchase All Upfront Reserved Instances with a 3-year term for Amazon RDS.

Answer: D

Explanation:

Question: 394

A company has a data ingestion workflow that consists the following:

An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries

An AWS Lambda function to process the data and record metadata

The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.

Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Select TWO.)

- A. Configure the Lambda function In multiple Availability Zones.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe It to me SNS topic.
- C. Increase the CPU and memory that are allocated to the Lambda function.
- D. Increase provisioned throughput for the Lambda function.
- E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue

Answer: C

Explanation:

Question: 395

A company has a three-tier application image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance tor the application layer, and a third EC2 instance for a MySQL database A solutions architect must design a scalable and nighty available solution mat requires the least amount of change to the application.

Which solution meets these requirement?

- A. Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table Use Amazon S3 to store and service users' images.
- B. Use toad-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS OB instance with multiple read replicas to serve users' images.
- C. Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use toad-balanced Multi-AZ AWS Elastic Beanstark environments for tie front-end layer and the application layer. Move the database to an Amazon ROS Multi-AZ DB instance Use Amazon S3 to store and serve users' images.

Answer: C

Explanation:

Question: 396

A company wants to share data that « collected from self-driving cars with the automobile community The data will be made available from within an Amazon S3 bucket The company wants to minimize its cost of making this data available to other AWS accounts.

What should a solutions architect do to accomplish this goal?

- A. Create an S3 VPC endpoint for me bucket
- B. Configure the S3 bucket to be a Requested Pays bucket
- C. Create an Amazon CloudFront distribution in front of the S3 bucket
- D. Require that the files be accesses only with the use of the BitTorrent protocol

Answer: B

Explanation:

Question: 397

A company is hosting its website on Amazon S3 and is using Amazon CloudFront to cache content The company has an upcoming product launch An employee accidentally published marketing content to the website before the official release of the product The company needs to remove the marketing content from the website as quickly as possible

Which solution will meet these requirements?

- A. Deploy the updated version of the website to another S3 bucket Update the origin for CloudFront
- B. Delete the marketing content in the existing S3 bucket Invalidate the file path in CloudFront
- C. Create a new CloudFront cache policy with a low TTL Associate the new policy with the existing CloudFront distribution
- D. Delete the marketing content in the existing S3 bucket Update the S3 bucket policy to block requests to the file path

Answer: B

Explanation:

Question: 398

A company is running a media application in an on-premises data center and has accumulated 500 TB of data The company needs to migrate the data from the application s existing network-attached file system to AWS Users rarely access data that is older than 1 year

Which solution meets these requirements MOST cost-effectively?

- A. Use AWS Snowmobile to move the data to Amazon S3 Create an S3 Lifecycle policy to transition data that is older than 1 year to S3 Glacier
- B. Use multiple AWS Snowball Edge Storage Optimized devices to move the data to Amazon S3 Create an S3 Lifecycle policy to transition data that is older than 1 year to S3 Standard-Infrequent Access (S3 Standard-IA)
- C. Set up an AWS Direct Connect connection between the on-premises data center and AWS Transfer the data directly to Amazon S3 by using the Direct Connect connection Create an S3 Lifecycle policy to transition data that is older than 1 year to S3 Glacier

D. Set up an AWS Site-to-Site VPN connection between the on-premises data center and AWS Transfer the data directly to Amazon S3 by using the Site-to-Site VPN connection Create an S3 Lifecycle policy to transition data that is older than 1 year to S3 Standard-infrequent Access (S3 Standard-IA)

Answer: A

Explanation:

Question: 399

A company needs to migrate a large amount of data from an on-premises storage area network (SAN) to Amazon S3 The SAN currently has 200 TB of data and is receiving an additional 20 TB of data each month The company has a 500 Mbps connection to the internet What should the company do to migrate the data to Amazon S3 in the LEAST amount of time?

- A. Use a file syncing application to sync the data to Amazon S3 over the internet through a public S3 endpoint Sync any changed data the same way until the SAN is decommissioned
- B. Use an AWS Snowball Edge Storage Optimized device to migrate the initial 200 TB of data to Amazon S3 Sync any changed data by using AWS DataSync until the SAN is decommissioned
- C. Set up an AWS Site-to-Site VPN connection Use a file syncing application to sync the data to Amazon S3 through a private S3 endpoint Sync any changed data the same way until the SAN is decommissioned
- D. Set up a 10 Gbps AWS Direct Connect connection Migrate the initial 200 TB of data to Amazon S3 by using a file syncing application Sync any changed data the same way until the SAN is decommissioned.

Answer: B

Explanation:

Question: 400

Which AWS service or feature can be used find availability status information on all AWS services?

- A. AWS Personal Health
- B. Dashboard AWS CloudTrail
- C. AWS Service Health Dashboard
- D. Amazon CloudWatch

Answer: A

Explanation:

Question: 401

Which AWS service can a company use to store and manage Docker images?

- A. Amazon DynamoDB

- B. Amazon Kinesis Data Streams
- C. Amazon Elastic Container Registry (Amazon ECR)
- D. Amazon Elastic File System (Amazon EFS)

Answer: C

Explanation:

Question: 402

A company wants to design its cloud architecture so that its workloads are resilient, can consistently perform their intended functions correctly, and can recover from failure quickly
Which pillar of the AWS Well-Architected Framework does this architecture represent?

- A. Security
- B. Performance efficiency
- C. Operational excellence
- D. Reliability

Answer: C

Explanation:

Question: 403

A company wants to minimize cost by moving infrequently accessed audit archives to low-cost storage.
Which AWS service should the company use for this storage?

- A. AWS Backup
- B. Amazon S3 Glacier
- C. AWS Snowball
- D. AWS Storage Gateway

Answer: B

Explanation:

Question: 404

A company with multiple accounts and teams wants to set up a new multi-account AWS environment.
Which AWS service supports this requirement?

- A. AWS CloudFormation
- B. AWS Control Tower
- C. AWS Config
- D. Amazon Virtual Private Cloud (Amazon VPC)

Answer: B

Explanation:

Question: 405

A company wants to track its daily AWS resource usage to avoid reaching service quotas unexpectedly. The company needs to receive notifications when any service quota is exceeded. Which combination of actions should a solutions architect take to meet this requirement? (Select TWO.)

- A. Configure Amazon Simple Notification Service (Amazon SNS) as the target to send notifications
- B. Use the DescribeTrustedAdvisorChecks API operation to get AWS Trusted Advisor Service Limits checks every 24 hours
- C. Create an AWS Lambda function that runs every 24 hours and refreshes the AWS Trusted Advisor Service Limits checks
- D. Use AWS Config to monitor the AWS resources service quotas and create a periodic invocation for an AWS Lambda function.
- E. Use Amazon EventBridge (Amazon CloudWatch Events) to capture the events. Configure Amazon Simple Notification Service (Amazon SNS) as the target

Answer: B, D

Explanation:

Question: 406

A solutions architect needs to connect a company's corporate network to its VPC to allow on-premises access to its AWS resources. The solution must provide encryption of all traffic between the corporate network and the VPC at the network layer and the session layer. The solution also must provide security controls to prevent unrestricted access between AWS and the on-premises systems. Which solution meets these requirements?

- A. Configure AWS Direct Connect to connect to the VPC. Configure the VPC route tables to allow and deny traffic between AWS and on premises as required
- B. Create an IAM policy to allow access to the AWS Management Console only from a defined set of corporate IP addresses. Restrict user access based on job responsibility by using an IAM policy and roles.
- C. Configure AWS Site-to-Site VPN to connect to the VPC. Configure route table entries to direct traffic from on premises to the VPC. Configure instance security groups and network ACLs to allow only required traffic from on premises.
- D. Configure AWS Transit Gateway to connect to the VPC. Configure route table entries to direct traffic from on premises to the VPC. Configure instance security groups and network ACLs to allow only required traffic from on premises.

Answer: D

Explanation:

Question: 407

A solutions architect is migrating a document management workload to AWS. The workload keeps 7 TiB of contract documents on a shared storage file system and tracks them on an external database. Most of the documents are stored and retrieved eventually for reference in the future. The application cannot be modified during the migration, and the storage solution must be highly available.

Documents are retrieved and stored by web servers that run on Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group can have up to 12 instances. Which solution meets these requirements MOST cost-effectively?

- A. Provision an enhanced networking optimized EC2 instance to serve as a shared NFS storage system.
- B. Create an Amazon S3 bucket that uses the S3 Standard-infrequent Access (S3 Standard-IA) storage class. Mount the S3 bucket to the EC2 instances in the Auto Scaling group.
- C. Create an SFTP server endpoint by using AWS Transfer for SFTP and an Amazon S3 bucket. Configure the EC2 instances in the Auto Scaling group to connect to the SFTP server.
- D. Create an Amazon Elastic File System (Amazon EFS) file system that uses the EFS Standard-Infrequent Access (EFS Standard-IA) storage class. Mount the file system to the EC2 instances in the Auto Scaling group.

Answer: A

Explanation:

Question: 408

A large media company hosts a web application on AWS. The company wants to start caching confidential media files so that users around the world will have reliable access to the files. The content is stored in Amazon S3 buckets. The company must deliver the content quickly, regardless of where the requests originate geographically.

Which solution will meet these requirements?

- A. Use AWS DataSync to connect the S3 buckets to the web application.
- B. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.
- C. Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.
- D. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.

Answer: C

Explanation:

Question: 409

A company asks a solutions architect to design a new network architecture for its on-premises applications. The company has five application VPCs. Each application VPC supports a different application. All the application VPCs need to reach a shared services VPC for enterprise services. The application VPCs need to communicate with each other.

The number of VPCs will increase as the company grows. The company needs a solution that minimizes operational overhead during setup and maintenance. Which solution will meet these requirements?

- A. Use VPC endpoint services from the application VPCs to reach services on the shared services VPC.
- B. Use VPC peering connections between the application VPCs and the shared services VPC. Add a peering connection and routes between the application VPCs as needed.
- C. Use AWS Transit Gateway to connect the shared services VPC to each of the application VPCs. Configure routing to allow the application VPCs to access the shared services network.
- D. Use a virtual private gateway and VPNs in each application VPC to reach the company network. Transfer the network traffic between the application VPCs by using dynamic routing to the on-premises network.

Answer: C

Explanation:

Question: 410

A company has migrated several applications to AWS in the past 3 months. The company wants to know the breakdown of costs for each of these applications. The company wants to receive a regular report that includes this information.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Budgets to download data for the past 3 months into a csv file. Look up the desired information.
- B. Load AWS Cost and Usage Reports into an Amazon RDS DB instance. Run SQL queries to get the desired information.
- C. Tag all the AWS resources with a key for cost and a value of the application's name. Activate cost allocation tags. Use Cost Explorer to get the desired information.
- D. Tag all the AWS resources with a key for cost and a value of the application's name. Use the AWS Billing and Cost Management console to download bills for the past 3 months. Look up the desired information.

Answer: C

Explanation:

Question: 411

A company is building a new data analysis application that will ingest large volumes of data into an Amazon S3 bucket. The company is concerned that sensitive information, such as personally identifiable information (PII), might be included in some of the data that is ingested. The company needs a solution that will scan for sensitive data and log the findings.

What should a solutions architect recommend to meet these requirements?

- A. Deploy Amazon Inspector to scan the ingested data. Configure Amazon Inspector to log findings to Amazon CloudWatch if Amazon Inspector finds any sensitive data.
- B. Deploy Amazon QuickSight to scan the ingested data. Configure QuickSight to log findings to

Amazon CloudWatch if QuickSight finds any sensitive data.

C. Create a series of AWS Lambda functions to call Amazon GuardDuty to perform scans of the ingested data. If GuardDuty finds any sensitive data, invoke a Lambda function to write findings to Amazon CloudWatch.

D. Create a series of AWS Lambda functions to call Amazon Macie to perform scans of the ingested data. If Macie finds any sensitive data, invoke a Lambda function to write findings to Amazon CloudWatch.

Answer: D

Explanation:

Question: 412

A company is migrating its application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster behind an Application Load Balancer (ALB). The disaster recovery (DR) requirements for the application include the ability to fail over to another AWS Region with minimal downtime.

Which combination of actions should a solutions architect take to meet this requirement? (Select TWO.)

A. Create a scaled-down clone environment in the DR Region. Use auto scaling policies with the EKS nodes.

B. Create an Amazon Route 53 record that points to the ALB. Configure an active-passive failover routing policy on the record.

C. Create an AWS Resource Access Manager policy that grants the application users access to the DR environment when the DR environment is needed.

D. Create an AWS Lambda function that monitors the availability of the main environment and deploys the DR environment when the DR environment is needed.

E. Create an AWS CloudFormation template that deploys the stack. Deploy the same template in the DR Region when the main environment is unavailable.

Answer: B, E

Explanation:

Question: 413

A company is building a shopping application on AWS. The application offers a catalog that changes once each month and needs to scale with traffic volume. The company wants the lowest possible latency from the application. Data from each user's shopping cart needs to be highly available. User session data must be available even if the user is disconnected and reconnects.

What should a solutions architect do to ensure that the shopping cart data is preserved at all times?

A. Configure an Application Load Balancer to enable the sticky sessions feature (session affinity) for access to the catalog in Amazon Aurora.

B. Configure Amazon ElastiCache for Redis to cache catalog data from Amazon DynamoDB and shopping cart data from the user's session.

C. Configure Amazon Elasticsearch Service (Amazon ES) to cache catalog data from Amazon DynamoDB and shopping cart data from the user's session.

D. Configure an Amazon EC2 instance with Amazon Elastic Block Store (Amazon EBS) storage for the catalog and shopping cart. Configure automated snapshots.

Answer: B

Explanation:

Question: 414

A company has an internet-facing application that runs on premises. The application contains mostly user-generated content. The data is stored in an on-premises network-attached storage system. The company wants to archive this data annually and has chosen to move the archival data to Amazon S3. The company needs a solution to migrate the archival data into an S3 bucket.

Which solution will meet these requirements?

- A. Use AWS Storage Gateway Volume Gateway. Cache the data, and then replicate the data from the on-premises environment to Amazon S3.
- B. Use AWS DataSync. Create a configuration to replicate the data from the on-premises environment to Amazon S3.
- C. Use AWS Transfer Family. Use an SFTP client to serially transfer the data from the on-premises environment to Amazon S3.
- D. Use Amazon S3 Transfer Acceleration. Use a third-party backup utility to replicate the data from the on-premises environment to Amazon S3.

Answer: B

Explanation:

Question: 415

A company has deployed an internal API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a VPC in a second account. The application is deployed in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected.

Which combination of architectural changes will reduce the NAT gateway costs? (Select TWO.)

- A. Configure a VPC peering connection between the two VPCs.
- B. Configure an AWS Direct Connect connection between the two VPCs.
- C. Replace the internet-facing ALB with an internal ALB. Access the API by using the ALB's private DNS address.
- D. Configure a ClassicLink connection for the API to the client VPC. Access the API by using the ClassicLink address.
- E. Configure an AWS Resource Access Manager connection between the two accounts. Access the API by using the ALB's private DNS address.

Answer: A,E

Explanation:

Question: 416

A company created and hosts a legacy software application for its customers. The application runs on a dedicated Linux server for each customer. The application stores no persistent data except for MySQL data.

The company experienced some data corruption issues in the past and wants to move the application to AWS. The company needs to implement a solution to optimize the stability of the application. The solution also must give the company the ability to restore a customer's database to a specific point in time. The company will migrate customer data by using AWS Database Migration Service (AWS DMS).

Which architecture should a solutions architect recommend to meet these requirements?

- A. Set up a shared Amazon Aurora database. Configure an Amazon EC2 launch template for each customer.
- B. Set up a shared Amazon Aurora database. Create an Amazon EC2 Amazon Machine Image (AMI) for each customer. Use the AMI to launch the application.
- C. Set up an Amazon RDS database and an Amazon EC2 instance for each customer. Download the installation script. Run the script to install and configure the application.
- D. Set up an Amazon RDS database for each customer. Deploy the application by using an Amazon EC2 launch template. Use user data to configure the customer-specific data.

Answer: C

Explanation:

Question: 417

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.

What should a solutions architect do to meet this requirement with the LEAST operational effort?

- A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.
- B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.
- C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.
- D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda

function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket

Answer: A

Explanation:

Question: 418

A company has a web application that users access from around the world. The company has web servers in multiple AWS Regions to support the traffic. A solutions architect must configure an Amazon Route 53 routing policy to send traffic to only the active web servers. Which configuration meets this requirement?

- A. Create a simple routing policy that uses health checks for each Region
- B. Create a multivalue answer routing policy that uses health checks for each Region
- C. Create a geoproximity routing policy with a health check bias of 99 for each Region
- D. Create a weighted routing policy with a health check weight of 100 for each Region

Answer: B

Explanation:

Question: 419

A company is running a critical business application on an Amazon EC2 instance. The EC2 instance is hosting an Apache web server and a MySQL database server. The application serves static content and dynamic content to end users. The application is experiencing severe availability issues because of heavy user demand. The company needs a solution that resolves the availability issues with the least operational effort and the least change to the application. What should a solutions architect do to meet these requirements?

- A. Deploy the application and the web server on AWS Fargate. Use a Network Load Balancer to route traffic. Migrate the database to Amazon DynamoDB.
- B. Create an Amazon Machine Image (AMI) from the current EC2 instance. Create an Auto Scaling group to provide more capacity as needed. Use a Network Load Balancer to route traffic.
- C. Host static content on Amazon S3. Deploy the application and the web server on AWS Fargate. Use an Application Load Balancer to route traffic. Migrate the database to Amazon Aurora Serverless.
- D. Host static content on Amazon S3. Deploy the application on EC2 instances that are configured in an Auto Scaling group. Use an Application Load Balancer to route traffic. Migrate the database to Amazon DynamoDB.

Answer: C

Explanation:

Question: 420

A company wants to move its on-premises network attached storage (NAS) to AWS. The company

wants to make the data available to any Linux instances within its VPC and ensure changes are automatically synchronized across all instances accessing the data store. The majority of the data is accessed very rarely, and some files are accessed by multiple users at the same time. Which solution meets these requirements and is MOST cost-effective?

- A. Create an Amazon Elastic Block Store (Amazon EBS) snapshot containing the data. Share it with users within the VPC.
- B. Create an Amazon S3 bucket that has a lifecycle policy set to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after the appropriate number of days.
- C. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the throughput mode to Provisioned and to the required amount of IOPS to support concurrent usage.
- D. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the lifecycle policy to transition the data to EFS Infrequent Access (EFS IA) after the appropriate number of days.

Answer: D

Explanation:

Question: 421

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3.
- B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

Answer: B, D

Explanation:

Question: 422

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.

- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database

Answer: A

Explanation:

Question: 423

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service Customer Master Keys (AWS KMS CMKs). A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Select TWO.)

- A. Attach the kms:decrypt permission to the Lambda function's resource policy.
- B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy.
- C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
- D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.
- E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

Answer: A, E

Explanation:

Question: 424

A company is building applications in containers. The company wants to migrate its on-premises development and operations services from its on-premises data center to AWS. Management states that production systems must be cloud agnostic and use the same configuration and administrative tools across all production systems. A solutions architect needs to design a managed solution that will align with open-source software.

Which solution meets these requirements?

- A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.
- B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS worker nodes.
- C. Launch the containers on Amazon Elastic Container Service (Amazon ECS) with AWS Fargate instances.
- D. Launch the containers on Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 instance worker nodes.

Answer: B

Explanation:

Question: 425

A company is planning to host its compute-intensive applications on Amazon EC2 instances. The majority of the network traffic will be between these applications. The company needs a solution that minimizes latency and maximizes network throughput. The underlying hardware for the EC2 instances must not be shared with any other company. Which solution will meet these requirements?

- A. Launch EC2 instances as Dedicated Hosts in a cluster placement group
- B. Launch EC2 instances as Dedicated Hosts in a partition placement group
- C. Launch EC2 instances as Dedicated Instances in a cluster placement group
- D. Launch EC2 instances as Dedicated Instances in a partition placement group

Answer: A

Explanation:

Question: 426

A company is running a web-based game in two Availability Zones in the us-west-2 Region. The web servers use an Application Load Balancer (ALB) in public subnets. The ALB has an SSL certificate from AWS Certificate Manager (ACM) with a custom domain name. The game is written in JavaScript and runs entirely in a user's web browser.

The game is increasing in popularity in many countries around the world. The company wants to update the application architecture and optimize costs without compromising performance.

What should a solutions architect do to meet these requirements?

- A. Use Amazon CloudFront and create a global distribution that points to the ALB. Reuse the existing certificate from ACM for the CloudFront distribution. Use Amazon Route 53 to update the application alias to point to the distribution.
- B. Use AWS CloudFormation to deploy the application stack to AWS Regions near countries where the game is popular. Use ACM to create a new certificate for each application instance. Use Amazon Route 53 with a geolocation routing policy to direct traffic to the local application instance.
- C. Use Amazon S3 and create an S3 bucket in AWS Regions near countries where the game is popular. Deploy the HTML and JavaScript files to each S3 bucket. Use ACM to create a new certificate for each S3 bucket. Use Amazon Route 53 with a geolocation routing policy to direct traffic to the local S3 bucket.
- D. Use Amazon S3 and create an S3 bucket in us-west-2. Deploy the HTML and JavaScript files to the S3 bucket. Use Amazon CloudFront and create a global distribution with the S3 bucket as the origin. Use ACM to create a new certificate for the distribution. Use Amazon Route 53 to update the application alias to point to the distribution.

Answer: A

Explanation:

Question: 427

A company serves a multilingual website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). This architecture is currently running in the us-west-1 Region but is exhibiting

high request latency for users located in other parts of the world

The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

How should a solutions architect accomplish this?

- A. Replace the existing architecture with a website served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to only cache based on the Accept-Language request header.
- C. Set up Amazon API Gateway with the ALB as an integration. Configure API Gateway to use an HTTP integration type. Set up an API Gateway stage to enable the API cache.
- D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the instances plus the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Answer: D

Explanation:

Question: 428

A company has media and application files that need to be shared internally. Users currently are authenticated using Active Directory and access files from a Microsoft Windows platform. The chief executive officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit.

What should a solutions architect recommend?

- A. Set up a corporate Amazon S3 bucket and move all media and application files.
- B. Configure Amazon FSx for Windows File Server and move all the media and application files.
- C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.
- D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes, and move all media and application files.

Answer: B

Explanation:

Question: 429

A company hosts an application on an AWS Lambda function that runs a number of processing steps. The Lambda function typically takes less than 5 minutes to run unless errors occur. The company needs to decouple the application code because of past errors that caused the whole process to fail when a processing step took longer than expected. The processing steps must be available to be replayed up to 12 months from when the original processing occurred.

How should a solutions architect design the new solution?

- A. Configure Amazon EventBridge (Amazon CloudWatch Events), and create an archive. Split the processes into separate Lambda functions. Create rules for the different event patterns from the Lambda functions to perform processing.

- B. Keep the Lambda function in place, but increase the timeout to 15 minutes Configure the Lambda function to write each processing step into an Amazon DynamoDB table Replay the steps by using a separate Lambda function and by querying the table when necessary
- C. Keep the Lambda function in place, but increase the timeout to 60 minutes. Configure the Lambda function to write each processing step into a daily file in an Amazon S3 bucket Replay the steps by using a separate Lambda function and by querying the file based on required date
- D. Configure Amazon Simple Queue Service (Amazon SQS) queues, and create an archive Split the processes into separate Lambda functions Pass messages to different queues as each process is completed, and invoke the next Lambda function to poll the queue for new messages Replay the messages from the SQL queue archive when necessary

Answer: D

Explanation:

Question: 430

A company is developing a video conversion application hosted on AWS The application will be available in two tiers: a free tier and a paid tier. Users in the paid tier will have their videos converted first and then the free tier users will have their videos converted

Which solution meets these requirements and is MOST cost-effective?

- A. One FIFO queue for the paid tier and one standard queue for the free tier
- B. A single FIFO Amazon Simple Queue Service (Amazon SQS) queue for all file types
- C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all file types
- D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier

Answer: A

Explanation:

Question: 431

A company is planning to migrate its virtual server-based workloads to AWS The company has internet-facing load balancers backed by application servers The application servers rely on patches from an internet-hosted repository

Which services should a solutions architect recommend be hosted on the public subnet? (Select TWO.)

- A. NAT gateway
- B. Amazon RDS DB instances
- C. Application Load Balancers
- D. Amazon EC2 application servers
- E. Amazon Elastic File System (Amazon EFS) volumes

Answer: A,D

Explanation:

Question: 432

A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels. The company has been experiencing application interruptions several times each day, resulting in lost transactions.

What should a solutions architect recommend to improve application resiliency?

- A. Modify the shipping application to write to a local database
- B. Modify the application APIs to run serverless using AWS Lambda
- C. Configure Amazon API Gateway to call the EC2 inventory application APIs
- D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS)

Answer: B

Explanation:

Question: 433

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.

Which solution meets these requirements'?

- A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL
- B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL
- C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
- D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Answer: A

Explanation:

Question: 434

A company needs a backup strategy for its three-tier stateless web application. The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events. The database tier runs on Amazon RDS for PostgreSQL. The web application does not require temporary local storage on the EC2 instances. The company's recovery point objective (RPO) is 2 hours.

The backup strategy must maximize scalability and optimize resource utilization for this environment. Which solution will meet these requirements?

- A. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO
- B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots Enable automated backups in Amazon RDS to meet the RPO
- C. Retain the latest Amazon Machine Images (AMIs) of the web and application tiers Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO
- D. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO

Answer: D

Explanation:

Question: 435

A company recently launched a new service that involves medical images. The company scans the images and sends them from its on-premises data center through an AWS Direct Connect connection to Amazon EC2 instances. After processing is complete, the images are stored in an Amazon S3 bucket. A company requirement states that the EC2 instances cannot be accessible through the internet. The EC2 instances run in a private subnet, which has a default route back to the on-premises data center for outbound internet access.

Usage of the new service is increasing rapidly. A solutions architect must recommend a solution that meets the company's requirements and reduces the Direct Connect charges.

Which solution accomplishes these goals MOST cost-effectively?

- A. Configure a VPC endpoint for Amazon S3. Add an entry to the private subnet's route table for the S3 endpoint.
- B. Configure a NAT gateway in a public subnet. Configure the private subnet's route table to use the NAT gateway.
- C. Configure Amazon S3 as a file system mount point on the EC2 instances. Access Amazon S3 through the mount.
- D. Move the EC2 instances into a public subnet. Configure the public subnet route table to point to an internet gateway.

Answer: B

Explanation:

Question: 436

A company is adopting serverless architecture. The company's solutions architect wants to modernize an application that has source data in CSV format. A large team of developers needs to use the application to run SQL queries and reports on demand by joining data across multiple tables.

Which combination of actions will meet these requirements MOST cost-effectively? (Select TWO)

- A. Store the source data in Amazon S3
- B. Load the source data into Amazon RDS
- C. Run on-demand reports and queries by using Amazon Athena
- D. Run on-demand reports and queries by using Amazon QuickSight

E. Run on-demand reports and queries by using Amazon DynamoDB

Answer: A, C

Explanation:

Question: 437

A company has an application that runs on Amazon EC2 instances within a private subnet in a VPC. The instances access data in an Amazon S3 bucket in the same AWS Region. The VPC contains a NAT gateway in a public subnet to access the S3 bucket. The company wants to reduce costs by replacing the NAT gateway without compromising security or redundancy. Which solution meets these requirements?

- A. Replace the NAT gateway with a NAT instance
- B. Replace the NAT gateway with an internet gateway
- C. Replace the NAT gateway with a gateway VPC endpoint
- D. Replace the NAT gateway with an AWS Direct Connect connection

Answer: C

Explanation:

Question: 438

A company needs to run its external website on Amazon EC2 instances and on-premises virtualized servers. The AWS environment has a 1 GB AWS Direct Connect connection to the data center. The application has IP addresses that will not change. The on-premises and AWS servers are able to restart themselves while maintaining the same IP address if a failure occurs. Some website users have to add their vendors to an allow list, so the solution must have a fixed IP address. The company needs a solution with the lowest operational overhead to handle this split traffic. What should a solutions architect do to meet these requirements?

- A. Deploy an Amazon Route 53 Resolver with rules pointing to the on-premises and AWS IP addresses
- B. Deploy a Network Load Balancer on AWS. Create target groups for the on-premises and AWS IP addresses
- C. Deploy an Application Load Balancer on AWS. Register the on-premises and AWS IP addresses with the target group
- D. Deploy Amazon API Gateway to direct traffic to the on-premises and AWS IP addresses based on the header of the request

Answer: B

Explanation:

Question: 439

A company allows users to upload and store photos through its website. The website has users from

all around the world. All images that users upload are stored in a centralized Amazon S3 bucket. The company wants to increase the speed in which its entire user base can upload photos through the website.

What should a solutions architect recommend to meet these requirements?

- A. Create an Amazon CloudFront distribution. Use the Amazon S3 Standard storage class to store files
- B. Create an Amazon CloudFront distribution. Configure the distribution settings and origin.
- C. Configure S3 Transfer Acceleration on the S3 bucket. Use the standard S3 endpoint to upload files
- D. Configure S3 Transfer Acceleration on the S3 bucket. Use the S3 Accelerate endpoint to upload files

Answer: D

Explanation:

Question: 440

A company runs an on-premises application. The company is planning to move the application to containers by using Kubernetes. The company wants to migrate the application to AWS to reduce the overhead of container infrastructure management. A solutions architect must configure the environment to allow deployment of the company's own custom Amazon Machine Image (AMI) to nodes.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Provision a Kubernetes cluster on Amazon EC2. Store container images in Docker Hub.
- B. Use AWS Fargate on Amazon Elastic Kubernetes Service (Amazon EKS). Store container images in Amazon Elastic Container Registry (Amazon ECR).
- C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with managed worker nodes. Store container images in Amazon Elastic Container Registry (Amazon ECR).
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with self-managed worker nodes. Store container images in an image repository that runs on Amazon EC2.

Answer: B

Explanation:

Question: 441

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application.

How can this be achieved?

- A. Create hourly snapshots of the production RDS DB instance.
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.
- C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Answer: B

Explanation:

Question: 442

A company is building a website that relies on reading and writing to an Amazon DynamoDB database. The website experiences high traffic during normal business hours, but the traffic declines drastically overnight and during weekends. The company is concerned about operating costs. Which solution will meet the website's traffic demands MOST cost-effectively?

- A. Enable DynamoDB Accelerator (DAX) to cache the data.
- B. Enable DynamoDB auto scaling when creating the tables.
- C. Enable Multi-AZ replication for the DynamoDB database.
- D. Enable DynamoDB on-demand capacity allocation when creating the tables.

Answer: D

Explanation:

Question: 443

A global company plans to track and store information about local allergens in an Amazon DynamoDB table and query this data from its website. The website traffic will fluctuate. The combined read capacity units (RCUs) and write capacity units (WCUs) will range from 10 per second to 10,000 per second, depending on the severity of the conditions for the given day. A solutions architect must design a solution that avoids throttling issues and manages capacity efficiently. The solution also must provide the ability to set a maximum number of capacity units.

What should the solutions architect do to meet these requirements?

- A. Use provisioned capacity mode. Set the table's maximum RCUs to 10,000.
- B. Use provisioned capacity mode. Configure a scaling policy in DynamoDB auto scaling.
- C. Use on-demand capacity mode. Set the table's maximum RCUs to 10,000.
- D. Use on-demand capacity mode for a couple of months. Then switch to provisioned capacity mode.

Answer: B

Explanation:

Question: 444

A company uses GPS trackers to document the migration patterns of thousands of sea turtles. The trackers check every 5 minutes to see if a turtle has moved more than 100 yards (91.4 meters). If a turtle has moved, its tracker sends the new coordinates to a web application running on three Amazon EC2 instances that are in multiple Availability Zones in one AWS Region. Recently, the web application was overwhelmed while processing an unexpected volume of tracker data. Data was lost with no way to replay the events. A solutions architect must prevent this problem from happening again and needs a solution with the least operational overhead.

What should the solutions architect do to meet these requirements"

- A. Create an Amazon S3 bucket to store the data Configure the application to scan for new data in the bucket for processing
- B. Create an Amazon API Gateway endpoint to handle transmitted location coordinates Use an AWS Lambda function to process each item concurrently
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue to store the incoming data Configure the application to poll for new messages for processing
- D. Create an Amazon DynamoDB table to store transmitted location coordinates Configure the application to query the table for new data for processing Use TTL to remove data that has been processed.

Answer: C

Explanation:

Question: 445

A company copies 200 TB of data from a recent ocean survey onto AWS Snowball Edge Storage Optimized devices The company has a high performance computing (HPC) cluster that is hosted on AWS to look for oil and gas deposits A solutions architect must provide the cluster with consistent sub-millisecond latency and high-throughput access to the data on the Snowball Edge Storage Optimized devices The company is sending the devices back to AWS Which solution will meet these requirements'?

- A. Create an Amazon S3 bucket Import the data into the S3 bucket. Configure an AWS Storage Gateway file gateway to use the S3 bucket Access the file gateway from the HPC cluster instances
- B. Create an Amazon S3 bucket Import the data into the S3 bucket Configure an Amazon FSx for Lustre file system and integrate it with the S3 bucket Access the FSx for Lustre file system from the HPC cluster instances
- C. Create an Amazon S3 bucket and an Amazon Elastic File System (Amazon EFS) file system Import the data into the S3 bucket Copy the data from the S3 bucket to the EFS file system Access the EFS file system from the HPC cluster instances
- D. Create an Amazon FSx for Lustre file system Import the data directly into the FSx for Lustre file system Access the FSx for Lustre file system from the HPC cluster instances

Answer: A

Explanation:

Question: 446

A company uses Amazon S3 as its object storage solution The company has thousands of S3 buckets it uses to store data Some of the S3 buckets have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented or are implemented partially: resulting in data being stored in high-cost storage Which solution will lower costs without compromising the availability of objects?

- A. Use S3 ACLs

- B. Use Amazon Elastic Block Store (Amazon EBS) automated snapshots
- C. Use S3 Intelligent-Tiering storage
- D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: C

Explanation:

Question: 447

A solutions architect finds that an Amazon Aurora cluster with On-Demand Instance pricing is being underutilized for a blog application. The application is used only for a few minutes several times each day for reads.

What should a solutions architect do to optimize utilization MOST cost-effectively?

- A. Enable Auto Scaling on the original Aurora database
- B. Convert the original Aurora database to Aurora parallel query
- C. Convert the original Aurora database to an Aurora global database
- D. Convert the original Aurora database to Amazon Aurora Serverless

Answer: A

Explanation:

Question: 448

A company has an application in which users create a large number of files. The company plans to migrate the application from its on-premises data center to AWS. Currently, the application uploads the files to a shared storage system. A separate fleet of servers then processes the files. Access to the files is controlled through Linux file system permissions.

The company needs to migrate the fleet of servers to Amazon EC2 instances. The company must maximize storage scalability and durability without changing the code of the existing application. Which solution will meet these requirements?

- A. Migrate the files to an Amazon S3 bucket. Mount the S3 bucket on the EC2 instances
- B. Migrate the files to a set of Amazon EC2 instance store volumes. Mount the instance store volumes on the EC2 instances
- C. Migrate the files to a set of Amazon Elastic Block Store (Amazon EBS) volumes. Mount the EBS volumes on the EC2 instances
- D. Migrate the files to an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on the EC2 instances

Answer: D

Explanation:

Question: 449

A company wants to replicate its data to AWS to recover in the event of a disaster. Today a system

administrator has scripts that copy data to an NFS share. Individual backup files need to be accessed with low latency by application administrators to deal with errors in processing. What should a solutions architect recommend to meet these requirements?

- A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share
- B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share
- C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share
- D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share

Answer: C

Explanation:

Question: 450

A financial services company wants to shut down two data centers and migrate more than 100 TB of data to AWS. The data has an intricate directory structure with millions of small files stored in deep hierarchies of subfolders. Most of the data is unstructured and the company's file storage consists of SMB-based storage types from multiple vendors. The company does not want to change its applications to access the data after migration.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

- A. Use AWS Direct Connect to migrate the data to Amazon S3 .
- B. Use AWS DataSync to migrate the data to Amazon FSx for Lustre
- C. Use AWS DataSync to migrate the data to Amazon FSx for Windows File Server
- D. Use AWS Direct Connect to migrate the data on-premises file storage to an AWS Storage Gateway volume gateway.

Answer: D

Explanation:

Question: 451

A company is using an Application Load Balancer (ALB) to present its application to the internet. The company finds abnormal traffic access patterns across the application. A solutions architect needs to improve visibility into the infrastructure to help the company understand these abnormalities better. What is the MOST operationally efficient solution that meets these requirements?

- A. Create a table in Amazon Athena for AWS CloudTrail logs. Create a query for the relevant information.
- B. Enable ALB access logging to Amazon S3. Create a table in Amazon Athena, and query the logs.
- C. Enable ALB access logging to Amazon S3. Open each file in a text editor, and search each line for

the relevant information

D. Use Amazon EMR on a dedicated Amazon EC2 instance to directly query the ALB to acquire traffic access log information

Answer: A

Explanation:

Question: 452

A company is designing a new multi-tier web application that consists of the following components:

- Web and application servers that run on Amazon EC2 instances as part of Auto Scaling groups
- An Amazon RDS DB instance for data storage

A solutions architect needs to limit access to the application servers so that only the web servers can access them. Which solution will meet these requirements?

- A. Deploy AWS PrivateLink in front of the application servers. Configure the network ACL to allow only the web servers to access the application servers.
- B. Deploy a VPC endpoint in front of the application servers. Configure the security group to allow only the web servers to access the application servers.
- C. Deploy a Network Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the network ACL to allow only the web servers to access the application servers.
- D. Deploy an Application Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the security group to allow only the web servers to access the application servers.

Answer: C

Explanation:

Question: 453

A company uses AWS to run all components of its three-tier web application. The company wants to automatically detect any potential security breaches within the environment. The company wants to track any findings and notify administrators if a potential breach occurs. Which solution meets these requirements?

- A. Set up AWS WAF to evaluate suspicious web traffic. Create AWS Lambda functions to log any findings in Amazon CloudWatch and send email notifications to administrators.
- B. Set up AWS Shield to evaluate suspicious web traffic. Create AWS Lambda functions to log any findings in Amazon CloudWatch and send email notifications to administrators.
- C. Deploy Amazon Inspector to monitor the environment and generate findings in Amazon CloudWatch. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to notify administrators by email.
- D. Deploy Amazon GuardDuty to monitor the environment and generate findings in Amazon CloudWatch. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule to publish a message to an Amazon Simple

Notification Service (Amazon SNS) topic to notify administrators by email

Answer: D

Explanation:

Question: 454

A company processes images into thumbnails and returns an email confirmation to the end user upon completion. The company's existing solution is facing performance bottlenecks and scalability issues. The company wants to migrate this process to AWS and implement a solution that requires the least possible configuration

Which solution meets these requirements?

A. Use Amazon S3 to store images and send notifications to AWS Lambda. Configure an AWS Lambda function to process the images into thumbnails, store the thumbnails in Amazon S3, and send an email confirmation through Amazon Simple Email Service (Amazon SES).

B. Use Amazon S3 to store images and send notifications to Amazon Simple Queue Service (Amazon SQS). Configure an Amazon EC2 instance to poll the SQS queue to process the images into thumbnails, store the thumbnails in Amazon S3, and send an email confirmation through Amazon Simple Email Service (Amazon SES).

C. Use Amazon S3 to store images and send notifications to Amazon Simple Notification Service (Amazon SNS). Configure Amazon SNS to invoke an AWS Lambda function to process the images into thumbnails, store the thumbnails in Amazon S3, and send an email confirmation through Amazon Simple Email Service (Amazon SES).

D. Use Amazon S3 to store images and send notifications to Amazon Simple Queue Service (Amazon SQS). Configure an AWS Lambda function to retrieve the messages from the SQS queue, process the images into thumbnails, store the thumbnails in Amazon S3, and send an email confirmation through Amazon Simple Email Service (Amazon SES).

Answer: C

Explanation:

Question: 455

A company runs an application on an Amazon EC2 instance. The application frequently writes and reads tens of thousands of intermediate computation results to disk. To finish within the allowed duration, the application must be able to complete all intermediate computations with sustained low latency.

Which Amazon Elastic Block Store (Amazon EBS) volume type should a solutions architect attach to the EC2 instance to meet these requirements?

- A. Cold HDD (sc1)
- B. General Purpose SSD (gp3)
- C. Provisioned IOPS SSD (io2)

D. Throughput Optimized HDD (st1)

Answer: C

Explanation:

Question: 456

A company hosts its enterprise content management platform in one AWS Region but needs to operate the platform across multiple Regions. The company has an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that runs its microservices. The EKS cluster stores and retrieves objects from Amazon S3. The EKS cluster also stores and retrieves metadata from Amazon DynamoDB. Which combination of steps should a solutions architect take to deploy the platform across multiple Regions? (Select TWO.)

- A. Replicate the EKS cluster with cross-Region replication.
- B. Use Amazon API Gateway to create a global endpoint to the EKS cluster.
- C. Use AWS Global Accelerator endpoints to distribute the traffic to multiple Regions.
- D. Use Amazon S3 access points to give access to the objects across multiple Regions. Configure DynamoDB Accelerator (DAX). Connect DAX to the relevant tables.
- E. Deploy an EKS cluster and an S3 bucket in another Region. Configure cross-Region replication on both S3 buckets. Turn on global tables for DynamoDB.

Answer: A, B

Explanation:

Question: 457

A company hosts a multi-tier web application on Amazon Linux Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The company observes that the Auto Scaling group launches more On-Demand Instances when the application's end users access high volumes of static web content. The company wants to optimize cost.

What should a solutions architect do to redesign the application MOST cost-effectively?

- A. Update the Auto Scaling group to use Reserved Instances instead of On-Demand Instances.
- B. Update the Auto Scaling group to scale by launching Spot Instances instead of On-Demand Instances.
- C. Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.
- D. Create an AWS Lambda function behind an Amazon API Gateway API to host the static website contents.

Answer: B

Explanation:

Question: 458

A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC. The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other. However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway. The company is concerned about data transfer charges.

What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

- A. Launch the NAT gateway in each Availability Zone
- B. Replace the NAT gateway with a NAT instance
- C. Deploy a gateway VPC endpoint for Amazon S3
- D. Provision an EC2 Dedicated Host to run the EC2 instances

Answer: A

Explanation:

Question: 459

A company wants to move from many standalone AWS accounts to a consolidated, multi-account architecture. The company plans to create many new AWS accounts for different business units. The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service.

Which combination of actions should a solutions architect recommend to meet these requirements? (Select TWO)

- A. Create a new organization in AWS Organizations with all features turned on. Create the new AWS accounts in the organization.
- B. Set up an Amazon Cognito identity pool. Configure AWS Single Sign-On to accept Amazon Cognito authentication.
- C. Configure a service control policy (SCP) to manage the AWS accounts. Add AWS Single Sign-On to AWS Directory Service.
- D. Create a new organization in AWS Organizations. Configure the organization's authentication mechanism to use AWS Directory Service directly.
- E. Set up AWS Single Sign-On (AWS SSO) in the organization. Configure AWS SSO and integrate it with the company's corporate directory service.

Answer: AB

Explanation:

Question: 460

A company hosts a three-tier web application that includes a PostgreSQL database. The database stores the metadata from documents. The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month. The documents are stored in Amazon S3. The documents are usually written only once, but they are updated frequently. The reporting

process takes a few hours with the use of relational queries. The reporting process must not affect any document modifications or the addition of new documents.

What are the MOST operationally efficient solutions that meet these requirements? (Select TWO)

- A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica. Scale the read replica to generate the reports.
- B. Set up a new Amazon RDS for PostgreSQL Reserved Instance and an On-Demand read replica. Scale the read replica to generate the reports.
- C. Set up a new Amazon Aurora PostgreSQL DB cluster that includes a Reserved Instance and an Aurora Replica. Issue queries to the Aurora Replica to generate the reports.
- D. Set up a new Amazon RDS for PostgreSQL Multi-AZ Reserved Instance. Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.
- E. Set up a new Amazon DynamoDB table to store the documents. Use a fixed write capacity to support new document entries. Automatically scale the read capacity to support the reports.

Answer: B, C

Explanation:

Question: 461

A solutions architect must secure a VPC network that hosts Amazon EC2 instances. The EC2 instances contain highly sensitive data and run in a private subnet. According to company policy, the EC2 instances must run in the VPC and can access only approved third-party software repositories on the internet for software product updates that use the third party's URL. Other internet traffic must be blocked.

Which solution meets these requirements?

- A. Update the route table for the private subnet to route the outbound traffic to an AWS Network Firewall. Configure domain list rule groups.
- B. Set up an AWS WAF web ACL. Create a custom set of rules that filter traffic requests based on source and destination IP address range sets.
- C. Implement strict inbound security group rules. Configure an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs.
- D. Configure an Application Load Balancer (ALB) in front of the EC2 instances. Direct an outbound traffic to the ALB. Use a URL-based rule listener in the ALB's target group for outbound access to the internet.

Answer: C

Explanation:

Question: 462

A company has a data ingestion workflow that includes the following components:

- An Amazon Simple Notification Service (Amazon SNS) topic that receives notifications about new data deliveries.

- An AWS Lambda function that processes and stores the data

The ingestion workflow occasionally fails because of network connectivity issues. When tenure occurs the corresponding data is not ingested unless the company manually reruns the job. What should a solutions architect do to ensure that all notifications are eventually processed?

- A. Configure the Lambda function (or deployment across multiple Availability Zones
- B. Modify the Lambda functions configuration to increase the CPU and memory allocations for the function
- C. Configure the SNS topic's retry strategy to increase both the number of retries and the wait time between retries
- D. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on failure destination. Modify the Lambda function to process messages in the queue

Answer: A

Explanation:

Question: 463

A company wants to migrate an on-premises data center to AWS. The data center hosts an SFTP server that stores its data on an NFS-based file system. The server holds 200 GB of data that needs to be transferred. The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system.

When combination of steps should a solutions architect take to automate this task? (Select TWO)

- A. Launch the EC2 instance into the same Availability Zone as the EFS file system
- B. Install an AWS DataSync agent in the on-premises data center
- C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data
- D. Manually use an operating system copy command to push the data to the EC2 instance
- E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server

Answer: CD

Explanation:

Question: 464

A company wants to relocate its on-premises MySQL database to AWS. The database accepts regular imports from a client-facing application when it causes a high volume of write operations. The company is concerned that the amount of traffic might be causing performance issues within the application.

How should a solutions architect design the architecture on AWS?

- A. Provision an Amazon RDS for MySQL DB instance with Provisioned IOPS SSD storage. Monitor write operation metrics by using Amazon CloudWatch. Adjust the provisioned IOPS if necessary.

- B. Provision an Amazon RDS for MySQL DB instance with General Purpose SSD storage. Place an Amazon ElastiCache cluster in front of the DB instance. Configure the application to query ElastiCache instead.
- C. Provision an Amazon DocumentDB (with MongoDB compatibility) instance with a memory optimized instance type. Monitor Amazon CloudWatch for performance-related issues. Change the instance class if necessary.
- D. Provision an Amazon Elastic File System (Amazon EFS) file system in General Purpose performance mode. Monitor Amazon CloudWatch for IOPS bottlenecks. Change to Provisioned Throughput performance mode if necessary.

Answer: A

Explanation:

Question: 465

A company runs a website that uses a content management system (CMS) on Amazon EC2. The CMS runs on a single EC2 instance and uses an Amazon Aurora MySQL Multi-AZ DB instance for the data. Website images are stored on an Amazon Elastic Block Store (Amazon EBS) volume that is mounted inside the EC2 instance.

Which combination of actions should a solutions architect take to improve the performance and resilience of the website? (Select TWO.)

- A. Move the website images into an Amazon S3 bucket that is mounted on every EC2 instance.
- B. Share the website images by using an NFS share from the primary EC2 instance. Mount this share on the other EC2 instances.
- C. Move the website images onto an Amazon Elastic File System (Amazon EFS) file system that is mounted on every EC2 instance.
- D. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an accelerator in AWS Global Accelerator for the website.
- E. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an Amazon CloudFront distribution for the website.

Answer: CE

Explanation:

Question: 466

A company uses a simple static website and wants to host it on AWS. The company already has a domain that it uses for email. The company needs a hosting solution that supports HTTPS. Which solution will meet these requirements MOST cost-effectively?

- A. Create an Amazon S3 bucket with a name to match the website. Upload the website to the S3 bucket. Set up website hosting for the S3 bucket. Set up the DNS to point to the S3 website endpoint.

- B. Create an Amazon S3 bucket upload the website to the S3 bucket. Set up an HTTPS certificate by using AWS Certificate Manager (ACM). Create an Amazon CloudFront distribution for the S3 bucket and choose Price Class All.
- C. Set up an open-source content management system (CMS) from AWS Marketplace Deploy the CMS across two Availability Zones Copy the website onto the CMS Set up the DNS to point to the CMS
- D. Create an Amazon S3 bucket Upload the website to the S3 bucket Set up an HTTPS certificate by using AWS Certificate Manager (ACM) Create an Amazon CloudFront distribution for the S3 bucket and choose Price Class 100 Point to the CloudFront distribution

Answer: D

Explanation:

Question: 467

A company needs to send large amounts of data from its data center to an Amazon S3 bucket on a regular basis. The data must be encrypted and must be transferred over a network that provides consistent bandwidth and low latency.

What should a solutions architect do to meet these requirements?

- A. Use an AWS Direct Connect connection
- B. Use an AWS VPN CloudHub connection
- C. Use HTTPS TLS for encryption of data in transit
- D. Use a gateway VPC endpoint to access Amazon S3

Answer: B

Explanation:

Question: 468

A company is planning to deploy a business-critical application in the AWS Cloud. The application requires durable storage with consistent, low-latency performance

Which type of storage should a solutions architect recommend to meet these requirements?

- A. Instance store volume
- B. Amazon ElastiCache for Memcached cluster
- C. Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume
- D. Throughput Optimized HDD Amazon Elastic Block Store (Amazon EBS) volume

Answer: C

Explanation:

Question: 469

A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a Network Load Balancer (NLB) in the us-west-2 Region Most of the company's users are located in the

United States and Europe The company wants to improve the performance and availability of the solution by using an AWS Region in Europe The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB Which solutions will allow traffic to be routed to all the EC2 instances? (Select TWO)

- A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs Create an Amazon CloudFront distribution Use the Route 53 record as the distribution's origin
- B. Create a standard accelerator by using AWS Global Accelerator Create endpoint groups in us-west-2 and eu-west-1 Add the two NLBs as endpoints for the endpoint groups
- C. Attach Elastic IP addresses to the six EC2 instances Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances Create an Amazon CloudFront distribution Use the Route 53 record as the distribution's origin.
- D. Create a standard accelerator by using AWS Global Accelerator Create endpoint groups in us-west-2 and eu-west-1 Add the six EC2 instances directly as endpoints for the endpoint groups Delete the NLBs
- E. Replace the two NLBs with two Application Load Balancers (ALBs) Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs Create an Amazon CloudFront distribution Use the Route 53 record as the distribution's origin

Answer: A, B

Explanation:

Question: 470

An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket Traffic must not traverse the internet How should a solutions architect configure access to meet these requirements?

- A. Create a private hosted zone by using Amazon Route 53
- B. Set up a gateway VPC endpoint for Amazon S3 in the VPC
- C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket
- D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket

Answer: B

Explanation:

Question: 471

A company experienced a breach that affected several applications in its on-premises data center The attacker took advantage of vulnerabilities in the custom applications that were running on the servers The company is now migrating its applications to run on Amazon EC2 instances The company wants to implement a solution that actively scans for vulnerabilities on the EC2 instances and sends a report that details the findings Which solution will meet these requirements?

- A. Deploy AWS Shield to scan the EC2 instances for vulnerabilities Create an AWS Lambda function to log any findings to AWS CloudTrail.

- B. Deploy Amazon Macie and AWS Lambda functions to scan the EC2 instances for vulnerabilities Log any findings to AWS CloudTrail
- C. Turn on Amazon GuardDuty Deploy the GuardDuty agents to the EC2 instances Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings
- D. Turn on Amazon Inspector Deploy the Amazon Inspector agent to the EC2 instances Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings

Answer: D

Explanation:

Question: 472

An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow A solutions architect needs to design an architecture for the order-processing application The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Step Functions to build the application.
- B. Integrate all the application components in an AWS Glue job
- C. Use Amazon Simple Queue Service (Amazon SQS) to build the application
- D. Use AWS Lambda functions and Amazon EventBridge (Amazon CloudWatch Events) events to build the application

Answer: B

Explanation:

Question: 473

A company runs multiple Amazon EC2 Linux instances in a VPC across two Availability Zones The instances host applications that use a hierarchical directory structure The applications need to read and write rapidly and concurrently to shared storage

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 bucket Allow access from all the EC2 instances in the VPC
- B. Create an Amazon Elastic File System (Amazon EFS) file system Mount the EFS file system from each EC2 instance
- C. Create a file system on a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume Attach the EBS volume to all the EC2 instances
- D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance Synchronize the EBS volumes across the different EC2 instances

Answer: B

Explanation:

Question: 474

A company used an Amazon RDS for MySQL DB instance during application testing. Before terminating the DB instance at the end of the test cycle, a solutions architect created two backups. The solutions architect created the first backup by using the mysqldump utility to create a database dump. The solutions architect created the second backup by enabling the final DB snapshot option on RDS termination.

The company is now planning for a new test cycle and wants to create a new DB instance from the most recent backup. The company has chosen a MySQL-compatible edition of Amazon Aurora to host the DB instance.

Which solutions will create the new DB instance? (Select TWO)

- A. Import the RDS snapshot directly into Aurora
- B. Upload the RDS snapshot to Amazon S3 then import the RDS snapshot into Aurora
- C. Upload the database dump to Amazon S3. Then import the database dump into Aurora.
- D. Use AWS Database Migration Service (AWS DMS) to import the RDS snapshot into Aurora.
- E. Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora.

Answer: A, C

Explanation:

Question: 475

A medical company is designing a new application that gathers symptoms from patients. The company has decided to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design. Data must be encrypted while at rest and in transit. Only authorized personnel of the company can access the data.

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO)

- A. Turn on server-side encryption on the SQS components. Update the default key policy to restrict key usage to a set of authorized principals.
- B. Turn on server-side encryption on the SNS components by using a custom CMK. Apply a key policy to restrict key usage to a set of authorized principals.
- C. Turn on encryption on the SNS components. Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic policy to allow only encrypted connections over TLS.
- D. Turn on server-side encryption on the SQS components by using a custom CMK. Apply a key policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.
- E. Turn on server-side encryption on the SQS components by using a custom CMK. Apply an IAM policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.

Answer: C, D

Explanation:

Question: 476

A solutions architect is designing a workload that will store hourly energy consumption by business tenants in a building. The sensors will feed a database through HTTP requests that will add up usage for each tenant. The solutions architect must use managed services when possible. The workload will receive more features in the future as the solutions architect adds independent components. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in an Amazon DynamoDB table.
- B. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon S3 bucket to store the processed data.
- C. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in a Microsoft SQL Server Express database on an Amazon EC2 instance.
- D. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon Elastic File System (Amazon EFS) shared file system to store the processed data.

Answer: A

Explanation:

Question: 477

A company is building a disaster recovery (DR) solution. The company wants to rotate its primary systems between AWS Regions on a regular basis. The company's application is geographically distributed and includes a serverless web tier. The application's database tier runs on Amazon Aurora. A solutions architect needs to build an architecture for the database layer to implement managed, planned failover. Which combination of actions will meet these requirements with the LEAST downtime*? (Select TWO.)

- A. Create an Aurora DB cluster. Configure Aurora Replicas.
- B. Fail over to one of the secondary DB clusters from another Region.
- C. Create an Aurora DB cluster snapshot. Restore from the snapshot.
- D. Configure an Aurora global database. Set up a secondary DB cluster.
- E. Promote one of the read replicas as a writer from the Amazon RDS console.

Answer: C, D

Explanation:

Question: 478

A company wants to migrate its 1 PB on-premises image repository to AWS. The images will be used

by a serverless web application Images stored in the repository are rarely accessed, but they must be immediately available Additionally, the images must be encrypted at rest and protected from accidental deletion

Which solution meets these requirements?

- A. Implement client-side encryption and store the images in an Amazon S3 Glacier vault Set a vault lock to prevent accidental deletion
- B. Store the images in an Amazon S3 bucket in the S3 Standard-Infrequent Access (S3 Standard-IA) storage class Enable versioning default encryption and MFA Delete on the S3 bucket.
- C. Store the images in an Amazon FSx for Windows File Server file share Configure the Amazon FSx file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share Use NTFS permission sets on the images to prevent accidental deletion
- D. Store the images in an Amazon Elastic File System (Amazon EFS) file share in the Infrequent Access storage class Configure the EFS file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share. Use NFS permission sets on the images to prevent accidental deletion

Answer: B

Explanation:

Question: 479

A company runs an application on several Amazon EC2 instances that store persistent data on an Amazon Elastic File System (Amazon EFS) file system. The company needs to replicate the data to another AWS Region by using an AWS managed service solution

Which solution will meet these requirements MOST cost-effectively'?

- A. Use the EFS-to-EFS backup solution to replicate the data to an EFS file system in another Region
- B. Run a nightly script to copy data from the EFS file system to an Amazon S3 bucket Enable S3 Cross-Region Replication on the S3 bucket
- C. Create a VPC in another Region Establish a cross-Region VPC peer Run a nightly rsync to copy data from the original Region to the new Region.
- D. Use AWS Backup to create a backup plan with a rule that takes a daily backup and replicates it to another Region Assign the EFS file system resource to the backup plan

Answer: D

Explanation:

Question: 480

A company is preparing to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database The company cannot migrate the database to a different engine because SQL Server features are used in the application's NET code The company wants to maximize availability and minimize operational overhead.

What should a solutions architect do to meet these requirements?

- A. Install SQL Server on Amazon EC2 in a Multi-AZ deployment

- B. Install SQL Server on Amazon EC2 in a spread placement group
- C. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment
- D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment

Answer: C

Explanation:

Question: 481

A doctor's office is moving all of its patient data to the AWS Cloud. The office needs to retain all the data indefinitely, but the data is rarely accessed after a year. The data must be immediately available during the first year. However, to minimize cost, the office is willing to wait a day for data that is more than 1 year old to become available.

Which combination of actions should a solutions architect take to meet these requirements MOST cost-effectively? (Select TWO)

- A. Create an Amazon S3 Lifecycle transition rule to move the data to S3 Glacier after a year
- B. Create an Amazon S3 Lifecycle transition rule to move the data to S3 Glacier Deep Archive after a year
- C. Create an Amazon S3 bucket for the data. Store data in the S3 bucket by using the S3 Glacier storage class
- D. Create an Amazon S3 bucket for the data. Store data in the bucket by using the S3 Standard storage class.
- E. Create an Amazon S3 bucket for the data. Store data in the bucket by using the S3 Intelligent-Tiering storage class

Answer: A, D

Explanation:

Question: 482

A company is deploying an application that processes large quantities of data in parallel. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to prevent groups of nodes from sharing the same underlying hardware.

Which networking solution meets these requirements?

- A. Run the EC2 instances in a spread placement group
- B. Group the EC2 instances in separate accounts
- C. Configure the EC2 instances with dedicated tenancy
- D. Configure the EC2 instances with shared tenancy.

Answer: A

Explanation:

Question: 483

A company manages a data lake in an Amazon S3 bucket that numerous applications share. The S3 bucket contains unique folders with a prefix for each application. The company wants to restrict each application to its specific folder and have granular control of the objects in each folder. Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Create dedicated S3 access points and access point policies for each application.
- B. Create an S3 Batch Operations job to set the ACL permissions for each object in the S3 bucket.
- C. Replicate the objects in the S3 bucket to new S3 buckets for each application. Create replication rules by prefix.
- D. Replicate the objects in the S3 bucket to new S3 buckets for each application. Create dedicated S3 access points for each application.

Answer: C

Explanation:

Question: 484

A social media company wants to allow its users to upload images in an application that is hosted in the AWS Cloud. The company needs a solution that automatically resizes the images so that the images can be displayed on multiple device types. The application experiences unpredictable traffic patterns throughout the day. The company is seeking a highly available solution that maximizes scalability.

What should a solutions architect do to meet these requirements?

- A. Create a static website hosted in Amazon S3 that invokes AWS Lambda functions to resize the images and store the images in an Amazon S3 bucket.
- B. Create a static website hosted in Amazon CloudFront that invokes AWS Step Functions to resize the images and store the images in an Amazon RDS database.
- C. Create a dynamic website hosted on a web server that runs on an Amazon EC2 instance. Configure a process that runs on the EC2 instance to resize the images and store the images in an Amazon S3 bucket.
- D. Create a dynamic website hosted on an automatically scaling Amazon Elastic Container Service (Amazon ECS) cluster that creates a resize job in Amazon Simple Queue Service (Amazon SQS). Set up an image-resizing program that runs on an Amazon EC2 instance to process the resize jobs.

Answer: A

Explanation:

Question: 485

A solutions architect must provide an automated solution for a company's compliance policy that states security groups cannot include a rule that allows SSH from 0.0.0.0/0. The company needs to be notified if there is any breach in the policy. A solution is needed as soon as possible. What should the solutions architect do to meet these requirements with the LEAST operational overhead?

- A. Write an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses and creates a notification every time it finds one
- B. Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.
- C. Create an IAM role with permissions to globally open security groups and network ACLs Create an Amazon Simple Notification Service (Amazon SNS) topic to generate a notification every time the role is assumed by a user
- D. Configure a service control policy (SCP) that prevents non-administrative users from creating or editing security groups. Create a notification in the ticketing system when a user requests a rule that needs administrator permissions

Answer: B

Explanation:

Question: 486

A company runs batch processes on Amazon EC2 instances that are needed only during business hours. These processes must preserve the data at all times but the speed of processing is not important. The company needs to run these processes in the MOST cost-effective manner. Which solution will meet these requirements?

- A. Use EC2 Reserved Instances with the All Upfront payment option
- B. Use EC2 Reserved instances with the Partial Upfront payment option
- C. Use Spot Fleet requests with the allocation strategy set to lowestPncc
- D. Use persistent Spot Instance requests with behaviour that stops interrupted instances

Answer: B

Explanation:

Question: 487

A company recently migrated its entire IT environment to the AWS Cloud. The company discovers that users are provisioning oversized Amazon EC2 instances and modifying security group rules without using the appropriate change control process. A solutions architect must devise a strategy to track and audit these inventory and configuration changes.

Which actions should the solutions architect take to meet these requirements? (Select TWO)

- A. Enable AWS CloudTrail and use it for auditing
- B. Use data lifecycle policies for the Amazon EC2 instances
- C. Enable AWS Trusted Advisor and reference the security dashboard
- D. Enable AWS Config and create rules for auditing and compliance purposes
- E. Restore previous resource configurations with an AWS CloudFormation template

Answer: A,D

Explanation:

Question: 488

A company is designing a message-driven order processing application on AWS. The application consists of many services and needs to communicate the results of its processing to multiple consuming services. Each of the consuming services may take up to 5 days to receive the messages. Which process will meet these requirements?

- A. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic. Each consuming service subscribes to this SNS topic and consumes the results.
- B. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic. Each consuming service consumes the messages directly from its corresponding SNS topic.
- C. The application sends the results of its processing to an Amazon Simple Queue Service (Amazon SQS) queue. Each consuming service runs as an AWS Lambda function that consumes this single SQS queue.
- D. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic. An Amazon Simple Queue Service (Amazon SQS) queue is created for each service, and each queue is configured to be a subscriber of the SNS topic.

Answer: C

Explanation:

Question: 489

A company uses an Amazon S3 bucket as its data lake storage platform. The S3 bucket contains a massive amount of data that is accessed randomly by multiple teams and hundreds of applications. The company wants to reduce its S3 storage costs and provide immediate availability for frequently accessed objects.

What is the MOST operationally efficient solution that meets these requirements?

- A. Create an S3 Lifecycle rule to transition objects to the S3 Intelligent-Tiering storage class.
- B. Store objects in Amazon S3 Glacier. Use S3 Select to provide applications with access to the data.
- C. Use data from S3 storage class analysis to create S3 Lifecycle rules to automatically transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class.
- D. Transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an AWS Lambda function to transition objects to the S3 Standard storage class when they are accessed by an application.

Answer: C

Explanation:

Question: 490

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted, and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups.

What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored.

- B. Modify the backup section of the database configuration to toggle the Enable encryption check box
- C. Create a snapshot of the database Copy it to an encrypted snapshot Restore the database from the encrypted snapshot
- D. Enable an encrypted read replica on RDS for MySQL Promote the encrypted read replica to primary Remove the original database instance

Answer: C

Explanation:

Question: 491

A company runs analytics software on Amazon EC2 instances. The software accepts job requests from users to process data that has been uploaded to Amazon S3 Users report that some submitted data is not being processed Amazon CloudWatch reveals that the EC2 instances have a consistent CPU utilization at of near 100%. The company wants to improve system performance and scale the system based on user load.

What should a solutions architect do to meet these requirements?

- A. Create a copy of the instance Place all instances behind an Application Load Balancer
- B. Create an S3 VPC endpoint for Amazon S3 Update the software to reference the endpoint
- C. Stop the EC2 instances Modify the instance type to one with a more powerful CPU and more memory Restart the instances
- D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS) Configure an EC2 Auto Scaling group based on queue size Update the software to read from the queue

Answer: C

Explanation:

Question: 492

A company is developing an API that mobile apps will use to retrieve weather information During beta testing the company ran the API on Amazon EC2 instances and used an Application Load Balancer (ALB) to route requests to a single Auto Scaling group The company used an Amazon DynamoDB table for persistent data storage

The company wants to move to an architecture that can scale easily with the least possible operational overhead

What should a solutions architect do to meet these requirements?

- A. Use separate Auto Scaling groups for each API request type Change the ALB to route requests to the appropriate Auto Scaling group
- B. Implement an Amazon API Gateway API to replace the ALB Configure each API request method with an AWS Lambda function to process the request
- C. Migrate the API to containers Use an Amazon Elastic Container Service (Amazon ECS) cluster that has services for each API request Configure each service with its own Auto Scaling group
- D. Configure the API to publish to an Amazon Simple Notification Service (Amazon SNS) topic for each API request method Subscribe an Amazon Simple Queue Service (Amazon SQS) queue to the

SNS topic Subscribe an AWS Lambda function to the SQS queue to process a request

Answer: B

Explanation:

Question: 493

An online gaming company is designing a game that is expected to be popular all over the world. A solutions architect needs to define an AWS Cloud architecture that supports near-real-time recording and displaying of current game statistics for each player along with the names of the top 25 players in the world at any given time.

Which AWS database solution and configuration should the solutions architect use to meet these requirements?

- A. Use Amazon RDS for MySQL as the data store for player activity. Configure the RDS DB instance for Multi-AZ support.
- B. Use Amazon DynamoDB as the data store for player activity. Configure DynamoDB Accelerator (DAX) for the player data.
- C. Use Amazon DynamoDB as the data store for player activity. Configure global tables in each required AWS Region for the player data.
- D. Use Amazon RDS for MySQL as the data store for player activity. Configure cross-Region read replicas in each required AWS Region based on player proximity.

Answer: B

Explanation:

Question: 494

A company is creating a three-tier web application consisting of a web server, an application server, and a database server. The application will track GPS coordinates of packages as they are being delivered. The application will update the database every 0.5 seconds.

The tracking will need to be read as fast as possible for users to check the status of their packages. Only a few packages might be tracked on some days, whereas millions of packages might be tracked on other days. Tracking will need to be searchable by tracking ID, customer ID, and order ID. Orders older than 1 month no longer need to be tracked.

What should a solutions architect recommend to accomplish this with minimal total cost of ownership?

- A. Use Amazon DynamoDB. Enable Auto Scaling on the DynamoDB table. Schedule an automatic deletion script for items older than 1 month.
- B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.
- C. Use an Amazon RDS On-Demand Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.
- D. Use an Amazon RDS Reserved Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.

Answer: B

Explanation:

Question: 495

A company has a remote factory that has unreliable connectivity. The factory needs to gather and process machine data and sensor data so that it can sense products on its conveyor belts and initiate a robotic movement to direct the products to the right location. Predictable low-latency compute processing is essential for the on-premises control systems. Which solution should the factory use to process the data?

- A. Amazon CloudFront lambda@Edge functions
- B. An Amazon EC2 instance that has enhanced networking enabled
- C. An Amazon EC2 instance that uses an AWS Global Accelerator endpoint
- D. An Amazon Elastic Block Store (Amazon EBS) volume on an AWS Snowball Edge cluster

Answer: A

Explanation:

Question: 496

A company has a serverless website with millions of objects in an Amazon S3 bucket. The company uses the S3 bucket as the origin for an Amazon CloudFront distribution. The company did not set encryption on the S3 bucket before the objects were loaded. A solutions architect needs to enable encryption for all existing objects and for all objects that are added to the S3 bucket in the future. Which solution will meet these requirements with the LEAST amount of effort?

- A. Create a new S3 bucket. Turn on the default encryption settings for the new S3 bucket. Download all existing objects to temporary local storage. Upload the objects to the new S3 bucket.
- B. Turn on the default encryption settings for the S3 bucket. Use the S3 Inventory feature to create a CSV file that lists the unencrypted objects. Run an S3 Batch Operations job that uses the copy command to encrypt those objects.
- C. Create a new encryption key by using AWS Key Management Service (AWS KMS). Change the settings on the S3 bucket to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Turn on versioning for the S3 bucket.
- D. Navigate to Amazon S3 in the AWS Management Console. Browse the S3 bucket's objects. Sort by the encryption field. Select each unencrypted object. Use the Modify button to apply default encryption settings to every unencrypted object in the S3 bucket.

Answer: C

Explanation:

Question: 497

A company is using Amazon CloudFront with its website. The company has enabled logging on the

CloudFront distribution, and logs are saved in one of the company's Amazon S3 buckets. The company needs to perform advanced analyses on the logs and build visualizations. What should a solutions architect do to meet these requirements'?

- A. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.
- C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- D. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.

Answer: B

Explanation:

Question: 498

A company is planning to migrate to AWS. The network layout will include more than 1,000 VPCs in a single AWS Region. The resources in the VPCs need to communicate with each other. What should a solutions architect recommend to meet these requirements?

- A. Create VPN tunnels from all the VPCs to each other. Enable route propagation.
- B. Create an AWS Direct Connect gateway and attach a public virtual interface (VIF) to each VPC. Enable route propagation.
- C. Peer all the VPCs together by creating and accepting peering requests. Update route tables with the new routes.
- D. Create a transit gateway and place attachments in subnets of all the VPCs. Configure a transit gateway route table with the new routes.

Answer: A

Explanation:

Question: 499

A company is hosting a high-traffic static website on Amazon S3 with an Amazon CloudFront distribution that has a default TTL of 0 seconds. The company wants to implement caching to improve performance for the website. However, the company also wants to ensure that stale content is not served for more than a few minutes after a deployment.

Which combination of caching methods should a solutions architect implement to meet these requirements? (Select TWO)

- A. Set the CloudFront default TTL to 2 minutes.
- B. Set a default TTL of 2 minutes on the S3 bucket.
- C. Add a Cache-Control private directive to the objects in Amazon S3.
- D. Create an AWS Lambda@Edge function to add an Expires header to HTTP responses. Configure the function to run on viewer response.

E. Add a Cache-Control max-age directive of 24 hours to the objects in Amazon S3. On deployment create a CloudFront invalidation to purge any changed files from edge caches

Answer: B, D

Explanation:

Question: 500

A company runs an infrastructure monitoring service. The company is building a new feature that will enable the service to monitor data in customer AWS accounts. The new feature will call AWS APIs in customer accounts to describe Amazon EC2 instances and read Amazon CloudWatch metrics. What should the company do to obtain access to customer accounts in the MOST secure way?

- A. Ensure that the customers create an IAM role in their account with read-only EC2 and CloudWatch permissions and a trust policy to the company's account
- B. Create a serverless API that implements a token vending machine to provide temporary AWS credentials for a role with read-only EC2 and CloudWatch permissions
- C. Ensure that the customers create an IAM user in their account with read-only EC2 and CloudWatch permissions. Encrypt and store customer access and secret keys in a secrets management system
- D. Ensure that the customers create an Amazon Cognito user in their account to use an IAM role with read-only EC2 and CloudWatch permissions. Encrypt and store the Amazon Cognito user and password in a secrets management system

Answer: A

Explanation:

Question: 501

A solutions architect is investigating AWS file storage solutions that can be used with a company's on-premises Linux servers and applications. The company has an existing VPN connection set up between the company's VPC and its on-premises network. Which AWS services should the solutions architect use? (Select TWO)

- A. AWS Backup
- B. AWS DataSync
- C. AWS Snowball Edge
- D. AWS Storage Gateway
- E. Amazon Elastic File System (Amazon EFS)

Answer: D, E

Explanation:

Question: 502

A company stores 200 GB of data each month in Amazon S3. The company needs to perform analytics on this data at the end of each month to determine the number of items sold in each state

region for the previous month

Which analytics strategy is MOST cost-effective for the company to use?

- A. Create an Amazon Elasticsearch Service (Amazon ES) cluster Query the data in Amazon ES Visualize the data by using Kibana
- B. Create a table in the AWS Glue Data Catalog Query the data in Amazon S3 by using Amazon Athena Visualize the data in Amazon QuickSight
- C. Create an Amazon EMR cluster Query the data by using Amazon EMR and store the results in Amazon S3 Visualize the data in Amazon QuickSight.
- D. Create an Amazon Redshift cluster Query the data in Amazon Redshift and upload the results to Amazon S3 Visualize the data in Amazon QuickSight

Answer: B

Explanation:

Question: 503

A company is testing an application that runs on an Amazon EC2 Linux instance. The instance contains a data volume of 500 GB that consists of a single Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

The application is now ready for production use and will be installed on multiple EC2 instances that run in an Auto Scaling group All instances need access to the data that was stored on the 500 GB volume. The company needs a highly available and fault-tolerant solution that does not introduce any significant changes to the applications code

Which solution meets these requirements?

- A. Provision an EC2 instance with NFS server software that is configured with a single 500 GB gp2 volume
- B. Use an Amazon FSx for Windows File Server file system that is configured as an SMB file store within a single Availability Zone
- C. Migrate the data into an Amazon S3 bucket Use an EC2 instance profile to access the contents of the bucket
- D. Use an Amazon Elastic File System (Amazon EFS) file system that is configured with the General Purpose performance mode

Answer: A

Explanation:

Question: 504

A company wants to deploy a new public web application on AWS The application includes a web server tier that uses Amazon EC2 instances The application also includes a database tier that uses an Amazon RDS for MySQL DB instance

The application must be secure and accessible for global customers that have dynamic IP addresses How should a solutions architect configure the security groups to meet these requirements'?

- A. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.

- 0/0) Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers
- B. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers
- C. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers
- D. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0 Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0)

Answer: A

Explanation:

Question: 505

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

- A. Use AWS Storage Gateway for files to store and process the video content
- B. Use AWS Storage Gateway for volumes to store and process the video content
- C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS)
- D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing

Answer: D

Explanation:

Question: 506

A company has several business systems that require access to data stored in a file share. The business systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company's legacy on-premises environments and with AWS.

Which services meet the business requirements? (Select TWO)

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon FSx for Windows
- D. Amazon S3
- E. AWS Storage Gateway file gateway

Answer: C, D

Explanation:

Question: 507

A company is using AWS Organizations with two AWS accounts Logistics and Sales. The Logistics account operates an Amazon Redshift cluster. The Sales account includes Amazon EC2 instances. The Sales account needs to access the Logistics account's Amazon Redshift cluster. What should a solutions architect recommend to meet this requirement MOST cost-effectively?

- A. Set up VPC sharing with the Logistics account as the owner and the Sales account as the participant to transfer the data
- B. Create an AWS Lambda function in the Logistics account to transfer data to the Amazon EC2 instances in the Sales account
- C. Create a snapshot of the Amazon Redshift cluster and share the snapshot with the Sales account. In the Sales account, restore the cluster by using the snapshot ID that is shared by the Logistics account
- D. Run COPY commands to load data from Amazon Redshift into Amazon S3 buckets in the Logistics account. Grant permissions to the Sales account to access the S3 buckets of the Logistics account

Answer: A

Explanation:

Question: 508

A company is planning to store data on Amazon RDS DB instances. The company must encrypt the data at rest.

What should a solutions architect do to meet this requirement?

- A. Create an encryption key and store the key in AWS Secrets Manager. Use the key to encrypt the DB instances
- B. Generate a certificate in AWS Certificate Manager (ACM). Enable SSL/TLS on the DB instances by using the certificate
- C. Create a customer master key (CMK) in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances
- D. Generate a certificate in AWS Identity and Access Management (IAM). Enable SSL/TLS on the DB instances by using the certificate

Answer: C

Explanation:

Question: 509

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL

encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

- A. Create a new SSL certificate using AWS Certificate Manager (ACM) install the ACM certificate on each instance
- B. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket Configure the EC2 instances to reference the bucket for SSL termination
- C. Create another EC2 instance as a proxy server Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances
- D. Import the SSL certificate into AWS Certificate Manager (ACM) Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM

Answer: D

Explanation:

Question: 510

An application running on an Amazon EC2 instance in VPC-A needs to access dies in another EC2 instance in VPC-B Both VPCs are in separate AWS accounts The network administrator needs to design a solution to enable secure access to EC2 instance in VPC-B from VPC-A The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

- A. Set up a VPC peering connection between VPC-A and VPC-B
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B
- C. Attach a virtual private gateway to VPC-B and enable routing from VPC-A
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-B

Answer: A

Explanation:

Question: 511

A company runs its production workload on an Amazon Aurora MySQL DB cluster that includes six Aurora Replicas The company wants near-real-time reporting queries from one of its departments to be automatically distributed across three of the Aurora Replicas Those three replicas have a different compute and memory specification from the rest of the DB cluster

Which solution meets these requirements?

- A. Create and use a custom endpoint for the workload
- B. Create a three-node cluster clone and use the reader endpoint
- C. Use any of the instance endpoints for the selected three nodes
- D. Use the reader endpoint to automatically distribute the read-only workload

Answer: A

Explanation:

Question: 512

A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.

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

Which statement should a solutions architect add to the policy to correct bucket access?

A)

```
  "Action": [
    "s3:*Object"
  ],
  "Resource": [
    "arn:aws:s3:::bucket-name/*"
  ],
  "Effect": "Allow"
```

B)

```
  "Action": [
    "s3:*"
  ],
  "Resource": [
    "arn:aws:s3:::bucket-name/*"
  ],
  "Effect": "Allow"
```

C)

```
  "Action": [
    "s3:DeleteObject"
  ],
  "Resource": [
    "arn:aws:s3:::bucket-name*"
  ],
  "Effect": "Allow"
```

D)

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 513

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

Which combination of actions should a solutions architect take to meet these requirements? (Select TWO)

- A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster
- B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones
- C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.
- D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.
- E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Answer: B, D

Explanation:

Question: 514

A mobile gaming company runs application servers on Amazon EC2 instances. The servers receive updates from players every 15 minutes. The mobile game creates a JSON object of the progress made in the game since the last update and sends the JSON object to an Application Load Balancer. As the mobile game is played, game updates are being lost. The company wants to create a durable way to get the updates in order.

What should a solutions architect recommend to decouple the system?

- A. Use Amazon Kinesis Data Streams to capture the data and store the JSON object in Amazon S3
- B. Use Amazon Kinesis Data Firehose to capture the data and store the JSON object in Amazon S3
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to capture the data and EC2 instances to process the messages in the queue
- D. Use Amazon Simple Notification Service (Amazon SNS) to capture the data and EC2 instances to process the messages sent to the Application Load Balancer

Answer: C

Explanation:

Question: 515

A company is using a content management system that runs on a single Amazon EC2 instance. The EC2 instance contains both the web server and the database software. The company must make its website platform highly available and must enable the website to scale to meet user demand. What should a solutions architect recommend to meet these requirements?

- A. Move the database to Amazon RDS, and enable automatic backups. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer in the Availability Zone and set the two instances as targets.
- B. Migrate the database to an Amazon Aurora instance with a read replica in the same Availability Zone as the existing EC2 instance. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer and set the two EC2 instances as targets.
- C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.
- D. Move the database to a separate EC2 instance and schedule backups to Amazon S3. Create an Amazon Machine Image (AMI) from the original EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

Answer: C

Explanation:

Question: 516

A company hosts a web application on multiple Amazon EC2 instances. The EC2 instances are in an Auto Scaling group that scales in response to user demand. The company wants to optimize cost savings without making a long-term commitment. Which EC2 instance purchasing option should a solutions architect recommend to meet these requirements?

- A. Dedicated Instances only
- B. On-Demand Instances only
- C. A mix of On-Demand instances and Spot Instances
- D. A mix of On-Demand instances and Reserved instances

Answer: A

Explanation:

Question: 517

A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for MySQL Multi-AZ DB instance.

The company wants to optimize customer session management during transactions. The application must store session data durably.

Which solutions will meet these requirements? (Select TWO.)

- A. Turn on the sticky sessions feature (session affinity) on the ALB.
- B. Use an Amazon DynamoDB table to store customer session information.
- C. Deploy an Amazon Cognito user pool to manage user session information.
- D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.
- E. Use AWS Systems Manager Application Manager in the application to manage user session information.

Answer: A, B

Explanation:

Question: 518

An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table. Both the EC2 instance and the DynamoDB table are in the same AWS account. A solutions architect must configure the necessary permissions.

Which solution will allow least privilege access to the DynamoDB table from the EC2 instance?

- A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance.
- B. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Add the EC2 instance to the trust relationship policy document to allow it to assume the role.
- C. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Store the credentials in an Amazon S3 bucket and read them from within the application code directly.
- D. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls.

Answer: A

Explanation:

Question: 519

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be

accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class

Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

Explanation:

Question: 520

A company has migrated a fleet of hundreds of on-premises virtual machines (VMs) to Amazon EC2 instances. The instances run a diverse fleet of Windows Server versions along with several Linux distributions. The company wants a solution that will automate inventory and updates of the operating systems. The company also needs a summary of common vulnerabilities of each instance for regular monthly reviews.

What should a solutions architect recommend to meet these requirements?

- A. Set up AWS Systems Manager Patch Manager to manage all the EC2 instances. Configure AWS Security Hub to produce monthly reports.
- B. Set up AWS Systems Manager Patch Manager to manage all the EC2 instances. Deploy Amazon Inspector, and configure monthly reports.
- C. Set up AWS Shield Advanced, and configure monthly reports. Deploy AWS Config to automate patch installations on the EC2 instances.
- D. Set up Amazon GuardDuty in the account to monitor all EC2 instances. Deploy AWS Config to automate patch installations on the EC2 instances.

Answer: B

Explanation:

Question: 521

A company has hundreds of Amazon EC2 Linux-based instances in the AWS Cloud. Systems administrators have used shared SSH keys to manage the instances. After a recent audit, the company's security team is mandating the removal of all shared keys. A solutions architect must design a solution that provides secure access to the EC2 instances.

Which solution will meet this requirement with the LEAST amount of administrative overhead?

- A. Use AWS Systems Manager Session Manager to connect to the EC2 instances.
- B. Use AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand.
- C. Allow shared SSH access to a set of bastion instances. Configure all other instances to allow only SSH access from the bastion instances.
- D. Use an Amazon Cognito custom authorizer to authenticate users. Invoke an AWS Lambda function to generate a temporary SSH key.

Answer: B

Explanation:

Question: 522

A company wants to implement a disaster recovery plan for its primary on-premises file storage volume. The file storage volume is mounted from an Internet Small Computer Systems Interface (iSCSI) device on a local storage server. The file storage volume holds hundreds of terabytes (TB) of data.

The company wants to ensure that end users retain immediate access to all file types from the on-premises systems without experiencing latency.

Which solution will meet these requirements with the LEAST amount of change to the company's existing infrastructure?

A. Provision an Amazon S3 File Gateway as a virtual machine (VM) that is hosted on premises. Set the local cache to 10 TB. Modify existing applications to access the files through the NFS protocol. To recover from a disaster, provision an Amazon EC2 instance and mount the S3 bucket that contains the files.

B. Provision an AWS Storage Gateway tape gateway. Use a data backup solution to back up all existing data to a virtual tape library. Configure the data backup solution to run nightly after the initial backup is complete. To recover from a disaster, provision an Amazon EC2 instance and restore the data to an Amazon Elastic Block Store (Amazon EBS) volume from the volumes in the virtual tape library.

C. Provision an AWS Storage Gateway Volume Gateway cached volume. Set the local cache to 10 TB. Mount the Volume Gateway cached volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

D. Provision an AWS Storage Gateway Volume Gateway stored volume with the same amount of disk space as the existing file storage volume. Mount the Volume Gateway stored volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

Answer: C

Explanation:

Topic 5, Exam Pool Jan 2022

Question: 523

A company uses an Amazon Aurora PostgreSQL DB cluster to store its critical data in the us-east-1 Region. The company wants to develop a disaster recovery plan to recover the database in the us-west-1 Region. The company has a recovery time objective (RTO) of 5 minutes and has a recovery point objective (RPO) of 1 minute.

What should a solutions architect do to meet these requirements?

- A. Create a read replica in us-west-1 Set the DB cluster to automaKaliy fail over to the read replica if the primary instance is not responding
- B Create an Aurora global database Sel us-west-1 as the secondary Region update connections to use the writer and reader endpomis as appropriate
- C. Set up a second Aurora DB cluster in us-west-1 Use logical replication to keep the databases synchronized Create an Amazon EvontBridgc (Amazon CloudWatch Events) rule to change the database endpoint rf the primary DB cluster does not respond.
- D. Use Aurora automated snapshots to store data in an Amazon S3 bucket Enable S3 Verswnmg. Configure S3 Cross-Region Replication to us-west-1 Create a second Aurora DB cluster in us-west-1 Create an Amazon EventBndge (Amazon CloudWatch Events) rule to restore the snapshot il the primary D8 cluster does not respond

Answer: B

Explanation:

Question: 524

A company has two VPCs named Management and Production The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

- A. Add a set of VPNs between the Management and Production VPCs
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Answer: C

Explanation:

https://docs.aws.amazon.com/vpn/latest/s2svpn/images/Multiple_Gateways_diagram.png

"To protect against a loss of connectivity in case your customer gateway device becomes unavailable, you can set up a second Site-to-Site VPN connection to your VPC and virtual private gateway by using a second customer gateway device." <https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-redundant-connection.html>

Question: 525

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambd

- a. The application's traffic recently spiked due to fraudulent requests from botnets.
- Which steps should a solutions architect take to block requests from unauthorized users? (Select

TWO.)

- A. Create a usage plan with an API key that it shared with genuine users only.
- B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses
- C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out
- D. Convert the existing public API to a private API Update the DNS records to redirect users to the new API endpoint
- E. Create an IAM role for each user attempting to access the API A user will assume the role when making the API call

Answer: C, D

Explanation:

Question: 526

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive. Which solution offers the MOST reliable data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Answer: B

Explanation:

These are some of the main use cases for AWS DataSync: • Data migration – Move active datasets rapidly over the network into Amazon S3, Amazon EFS, or FSx for Windows File Server. DataSync includes automatic encryption and data integrity validation to help make sure that your data arrives securely, intact, and ready to use.

"DataSync includes encryption and integrity validation to help make sure your data arrives securely, intact, and ready to use." <https://aws.amazon.com/datasync/faqs/>

Question: 527

A company's infrastructure consists of hundreds of Amazon EC2 instances that use Amazon Elastic Block Store (Amazon EBS) storage. A solutions architect must ensure that every EC2 instance can be recovered after a disaster

What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Take a snapshot of the EBS storage that is attached to each EC2 instance Create an AWS CloudFormation template to launch new EC2 instances from the EBS storage.
- B. Take a snapshot of the EBS storage that is attached to each EC2 instance. Use AWS Elastic Beanstalk to set the environment based on the EC2 template and attach the EBS storage.

- C. Use AWS Backup to set up a backup plan for the entire group of EC2 instances. Use the AWS Backup API or the AWS CLI to speed up the restore process for multiple EC2 instances
- D. Create an AWS Lambda function to take a snapshot of the EBS storage that is attached to each EC2 instance and copy the Amazon Machine Images (AMIs). Create another Lambda function to perform the restores with the copied AMIs and attach the EBS storage.

Answer: C

Explanation:

Question: 528

A company is designing a distributed application to optimize its global supply chain and manufacturing process. The company has facilities near the us-east-1 Region, the eu-west-1 Region and the ap-south 1 Region.

According to the application requirements, orders that are booked in one Region must be visible in the other two Regions in 1 second or less. The database must be able to support failover with a recovery time objective (RTO) of less than 5 minutes. The application must avoid downtime so that the manufacturing process is not negatively affected

Which solution meets these requirements?

- A. Use Amazon DynamoDB to invoke an AWS Lambda function
- B. Use an Amazon Aurora global database
- C. Use Amazon RDS for MySQL with a cross-Region read replica
- D. Use Amazon RDS for PostgreSQL with a cross-Region read replica.

Answer: A

Explanation:

Question: 529

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company. How should security groups be configured in this situation? (Select TWO)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Answer: A,C

Explanation:

"Security groups create an outbound rule for every inbound rule." Not completely right. Stateful does NOT mean that if you create an inbound (or outbound) rule, it will create an outbound (or inbound) rule. What it does mean is: suppose you create an inbound rule on port 443 for the X ip. When a request enters on port 443 from X ip, it will allow traffic out for that request in the port 443. However, if you look at the outbound rules, there will not be any outbound rule on port 443 unless explicitly create it. In ACLs, which are stateless, you would have to create an inbound rule to allow incoming requests and an outbound rule to allow your application responds to those incoming requests.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#SecurityGroupRules

Question: 530

A company is running a high performance computing (HPC) workload on AWS across many Linux based Amazon EC2 instances. The company needs a shared storage system that is capable of sub-millisecond latencies, hundreds of Gbps of throughput and millions of IOPS. Users will store millions of small files.

Which solution meets these requirements?

- A. Create an Amazon Elastic File System (Amazon EFS) file system Mount the file system on each of the EC2 instances
- B. Create an Amazon S3 bucket Mount the S3 bucket on each of the EC2 instances
- C. Ensure that the EC2 instances use Amazon Elastic Block Store (Amazon EBS) optimized Mount Provisioned IOPS SSD (io2) EBS volumes with Multi-Attach on each instance
- D. Create an Amazon FSx for Lustre file system. Mount the file system on each of the EC2 instances

Answer: D

Explanation:

Question: 531

To meet security requirements, a company needs to encrypt all of its application data in transit while communicating with an Amazon RDS MySQL DB instance. A recent security audit revealed that encryption at rest is enabled using AWS Key Management Service (AWS KMS), but data in transit is not enabled.

What should a solutions architect do to satisfy the security requirements?

- A. Enable IAM database authentication on the database.
- B. Provide self-signed certificates, Use the certificates in all connections to the RDS instance
- C. Take a snapshot of the RDS instance Restore the snapshot to a new instance with encryption enabled
- D. Download AWS-provided root certificates Provide the certificates in all connections to the RDS instance

Answer: C

Explanation:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.E>

[ncryption.Enabling](#)

Question: 532

A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users.

The application has increased in popularity, and millions of users worldwide are accessing these media files. The company wants to provide the files to the users while reducing the load on the origin. Which solution meets these requirements MOST cost-effectively?

- A. Deploy an AWS Global Accelerator accelerator in front of the web servers
- B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket
- C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers
- D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers

Answer: B

Explanation:

CloudFront uses Edge Locations to cache content while Global Accelerator uses Edge Locations to find an optimal pathway to the nearest regional endpoint.

Question: 533

A company's order fulfillment service uses a MySQL database. The database needs to support a large number of concurrent queries and transactions. Developers are spending time patching and tuning the database. This is causing delays in releasing new product features.

The company wants to use cloud-based services to help address this new challenge. The solution must allow the developers to migrate the database with little or no code changes and must optimize performance.

Which service should a solutions architect use to meet these requirements'?

- A. Amazon Aurora
- B. Amazon DynamoDB
- C. Amazon ElastiCache
- D. MySQL on Amazon EC2

Answer: A

Explanation:

Amazon Aurora is managed DB and supports MySQL database.

<https://aws.amazon.com/rds/aurora/?aurora-whats-new.sort-by=item.additionalFields.postDateTime&aurora-whats-new.sort-order=desc>

Question: 534

A public-facing web application queries a database hosted on a Amazon EC2 instance in a private subnet. A large number of queries involve multiple table joins, and the application performance has been degrading due to an increase in complex queries. The application team will be performing updates to improve performance.

What should a solutions architect recommend to the application team? (Select TWO.)

- A. Cache query data in Amazon SQS
- B. Create a read replica to offload queries
- C. Migrate the database to Amazon Athena
- D. Implement Amazon DynamoDB Accelerator to cache data.
- E. Migrate the database to Amazon RDS

Answer: B, E

Explanation:

Question: 535

A company is running an application in a private subnet in a VPC with an attached internet gateway. The company needs to provide the application access to the internet while restricting public access to the application. The company does not want to manage additional infrastructure and wants a solution that is highly available and scalable.

Which solution meets these requirements?

- A. Create a NAT gateway in the private subnet. Create a route table entry from the private subnet to the internet gateway.
- B. Create a NAT gateway in a public subnet. Create a route table entry from the private subnet to the NAT gateway.
- C. Launch a NAT instance in the private subnet. Create a route table entry from the private subnet to the internet gateway.
- D. Launch a NAT instance in a public subnet. Create a route table entry from the private subnet to the NAT instance.

Answer: A

Explanation:

Question: 536

A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts. The company has created a central AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users. The solution must be secure and optimized.

How should a solutions architect meet these requirements?

- A. Configure an AWS Lambda function in each developer account to copy the log files to the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.

- B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account Create an IAM user in the central account for the auditor Attach an IAM policy providing full permissions to the bucket
- C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account Create an IAM role in the central account for the auditor Attach an IAM policy providing read-only permissions to the bucket
- D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account Create an IAM user in the central account for the auditor Attach an IAM policy providing full permissions to the bucket

Answer: C

Explanation:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-sharing-logs.html>

Question: 537

A company wants to build a scalable key management Infrastructure to support developers who need to encrypt data in their applications.

What should a solutions architect do to reduce the operational burden?

- A. Use multifactor authentication (MFA) to protect the encryption keys.
- B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys
- C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys
- D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys

Answer: B

Explanation:

Question: 538

A ride-sharing company stores historical service usage data as structured csv data files in Amazon S3 A data analyst needs to perform SQL queries on this data A solutions architect must recommend a solution that optimizes cost-effectiveness for the queries Which solution meets these requirements?

- A. Create an Amazon EMR cluster Load the data Perform the queries
- B. Create an Amazon Redshift cluster import the data Perform the queries
- C. Create an Amazon Aurora PostgreSQL DB cluster Import the data Perform the queries
- D. Create an Amazon Athena database Associate the data in Amazon S3 Perform the queries

Answer: D

Explanation:

<https://searchcloudcomputing.techtarget.com/answer/Compare-EMR-Redshift-and-Athena-for-data-analysis-on-AWS>

Question: 539

A company has deployed a server less application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket. The application uses the Lambda function to process the documents. After a recent marketing campaign, the company noticed that the application did not process many of the documents.

What should a solutions architect do to improve the architecture of this application?

- A. Set the Lambda function's runtime timeout value to 15 minutes
- B. Configure an S3 bucket replication policy. Stage the documents in the S3 bucket for later processing
- C. Deploy an additional Lambda function. Load balance the processing of the documents across the two Lambda functions
- D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.

Answer: B

Explanation:

Question: 540

A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.

How can the solutions architect meet this requirement?

- A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it
- B. Deploy a NAT gateway into a public subnet and attach an endpoint policy that allows access to the S3 buckets
- C. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets
- D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets

Answer: D

Explanation:

Question: 541

A company is running an ASP.NET MVC application on a single Amazon EC2 instance. A recent increase in application traffic is causing slow response times for users during lunch hours. The company needs to resolve this concern with the least amount of configuration.

What should a solutions architect recommend to meet these requirements?

- A. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling and time-based scaling to handle scaling during lunch hours
- B. Move the application to Amazon Elastic Container Service (Amazon ECS) Create an AWS Lambda function to handle scaling during lunch hours.
- C. Move the application to Amazon Elastic Container Service (Amazon ECS). Configure scheduled scaling for AWS Application Auto Scaling during lunch hours.
- D. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling, and create an AWS Lambda function to handle scaling during lunch hours.

Answer: A

Explanation:

- Scheduled scaling is the solution here, while "using the least amount of settings possible" - Beanstalk vs moving to ECS - ECS requires MORE CONFIGURATION / SETTINGS (task and service definitions, configuring ECS container agent) than Beanstalk (upload application code)

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-autoscaling-scheduledactions.html>

Elastic Beanstalk supports time based scaling, since we are aware that the application performance slows down during the lunch hours. <https://aws.amazon.com/about-aws/whats-new/2015/05/aws-elastic-beanstalk-supports-time-based-scaling/>

Question: 542

A company is expecting rapid growth in the near future. A solutions architect needs to configure existing users and grant permissions to new users on AWS The solutions architect has decided to create IAM groups The solutions architect will add the new users to IAM groups based on department

Which additional action is the MOST secure way to grant permissions to the new users?

- A. Apply service control policies (SCPs) to manage access permissions
- B. Create IAM roles that have least privilege permission Attach the roles to the IAM groups
- C. Create an IAM policy that grants least privilege permission Attach the policy to the IAM groups
- D. Create IAM roles Associate the roles with a permissions boundary that defines the maximum permissions

Answer: C

Explanation:

Question: 543

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

- A. S3 Standard

- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

Explanation:

Question: 544

A company has two AWS accounts in the same AWS Region. One account is a publisher account, and the other account is a subscriber account. Each account has its own Amazon S3 bucket.

An application puts media objects into the publisher account's S3 bucket. The objects are encrypted with server-side encryption with customer-provided encryption keys (SSE-C). The company needs a solution that will automatically copy the objects to the subscriber's account's S3 bucket.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Enable S3 Versioning on the publisher account's S3 bucket. Configure S3 Same-Region Replication of the objects to the subscriber account's S3 bucket.
- B. Create an AWS Lambda function that is invoked when objects are published in the publisher account's S3 bucket. Configure the Lambda function to copy the objects to the subscriber account's S3 bucket.
- C. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function when objects are published in the publisher account's S3 bucket. Configure the Lambda function to copy the objects to the subscriber account's S3 bucket.
- D. Configure Amazon EventBridge (Amazon CloudWatch Events) to publish Amazon Simple Notification Service (Amazon SNS) notifications when objects are published in the publisher account's S3 bucket. When notifications are received, use the S3 console to copy the objects to the subscriber account's S3 bucket.

Answer: B

Explanation:

Question: 545

A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet. An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets.

Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.

What should the solutions architect recommend to meet this requirement?

- A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.
- B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses

that are consuming resources.

C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.

D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

Answer: B

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison

Question: 546

A company has a document management application that contains PDF documents. The company hosts the application on Amazon EC2 instances. According to regulations, the instances must not have access to the internet. The application must be able to read and write to a persistent storage system that provides native versioning capabilities.

A solutions architect needs to design secure storage that maximizes resiliency and facilitates data sharing across instances.

Which solution meets these requirements?

A. Place the instances in a public subnet. Use Amazon S3 for storage. Access S3 objects by using URLs.

B. Place the instances in a private subnet. Use Amazon S3 for storage. Use a VPC endpoint to access S3 objects.

C. Use the instances with a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume.

D. Use Amazon Elastic File System (Amazon EFS) Standard-Infrequent Access (Standard-IA) to store data and provide shared access to the instances.

Answer: B

Explanation:

Question: 547

A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL Injection and also wants to detect and mitigate large, sophisticated DDoS attacks.

Which combination of solutions provides the MOST protection? (Select TWO.)

A. Use AWS WAF to protect the NLB.

B. Use AWS Shield Advanced with the NLB.

C. Use AWS WAF to protect Amazon API Gateway.

D. Use Amazon GuardDuty with AWS Shield Standard.

D. Use AWS Shield Standard with Amazon API Gateway.

Answer: A, B

Explanation:

Question: 548

A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPU Utilization metrics are spiking when monthly reports run. What is the MOST cost-effective solution?

- A. Migrate the monthly reporting to Amazon Redshift.
- B. Migrate the monthly reporting to an Aurora Replica
- C. Migrate the Aurora database to a larger instance class
- D. Increase the Provisioned IOPS on the Aurora instance

Answer: B

Explanation:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>
#Aurora.Replication.Replicas Aurora Replicas have two main purposes. You can issue queries to them to scale the read operations for your application. You typically do so by connecting to the reader endpoint of the cluster. That way, Aurora can spread the load for read-only connections across as many Aurora Replicas as you have in the cluster. Aurora Replicas also help to increase availability. If the writer instance in a cluster becomes unavailable, Aurora automatically promotes one of the reader instances to take its place as the new writer.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html>

Question: 549

A company runs a two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS D8 instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available. Which combination of configuration options will meet these requirements? (Select TWO.)

- A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
- B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
- C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
- D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.

E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones Deploy an Application Load Balancer in the public subnets

Answer: AE

Explanation:

Question: 550

A solution architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications. Which action should the solutions architect take?

- A. Configure a CloudFront signed URL.
- B. Configure a CloudFront signed cookie.
- C. Configure a CloudFront field-level encryption profile.
- D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.

Answer: C

Explanation:

Question: 551

A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket. What should the solutions architect do to meet this requirement?

- A. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.
- B. Create an IAM policy that grants access to the S3 bucket. Attach the policy to the EC2 instances.
- C. Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.
- D. Create an IAM user that grants access to the S3 bucket. Attach the user account to the EC2 instances.

Answer: C

Explanation:

Question: 552

A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability. The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours the company's development team pulls a full export of the production database to

populate a database in the staging environment During this period, users experience unacceptable application latency The development team is unable to use the staging environment until the procedure completes

A solutions architect must recommend replacement architecture that alleviates the application latency issue The replacement architecture also must give the development team the ability to continue using the staging environment without delay

Which solution meets these requirements?

- A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
- B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production Use database cloning to create the staging database on-demand
- C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production Use the standby instance for the staging database.
- D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

Answer: C

Explanation:

Question: 553

The DNS provider that hosts a company's domain name records is experiencing outages that cause service disruption for a website running on AWS The company needs to migrate to a more resilient managed DNS service and wants the service to run on AWS.

What should a solutions architect do to rapidly migrate the DNS hosting service?

- A. Create an Amazon Route 53 public hosted zone for the domain name. Import the zone file containing the domain records hosted by the previous provider.
- B. Create an Amazon Route 53 private hosted zone for the domain name Import the zone file containing the domain records hosted by the previous provider
- C. Create a Simple AD directory in AWS. Enable zone transfer between the DNS provider and AWS Directory Service for Microsoft Active Directory for the domain records.
- D. Create an Amazon Route 53 Resolver inbound endpoint in the VPC Specify the IP addresses that the provider's DNS will forward DNS queries to Configure the provider's DNS to forward DNS queries for the domain to the IP addresses that are specified in the inbound endpoint.

Answer: B

Explanation:

Question: 554

A company uses Amazon API Gateway to manage its REST APIs that third-party service providers access. The company must protect the REST APIs from SQL injection and cross site scripting attacks What is the MOST operationally efficient solution that meets these requirements?

- A. Configure AWS Shield
- B. Configure AWS WAF
- C. Set up API Gateway with an Amazon CloudFront distribution Configure AWS Shield in CloudFront
- D. Set up API Gateway with an Amazon CloudFront distribution Configure AWS WAF in CloudFront.

Answer: B

Explanation:

Question: 555

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries. Which policy should be used to meet this requirement?

- A. Simple routing policy
- B. Latency routing policy
- C. Multivalue routing policy
- D. Geolocation routing policy

Answer: C

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/> "Use a multivalue answer routing policy to help distribute DNS responses across multiple resources. For example, use multivalue answer routing when you want to associate your routing records with a Route 53 health check."

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-multivalue>

Question: 556

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone placing both behind an Application Load Balancer. After completing this change, users reported that, each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Answer: C

Explanation:

Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and

4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Redhat, and Ubuntu

AMIs, in conjunction with the Amazon EFS Mount Helper. For instructions, see Using the amazon-efs-utils Tools.

For a list of Amazon EC2 Linux Amazon Machine Images (AMIs) that support this protocol, see NFS Support. For some AMIs, you'll need to install an NFS client to mount your file system on your Amazon EC2 instance. For instructions, see Installing the NFS Client.

You can access your Amazon EFS file system concurrently from multiple NFS clients, so applications that scale beyond a single connection can access a file system. Amazon EC2 instances running in multiple Availability Zones within the same AWS Region can access the file system, so that many users can access and share a common data source.

Question: 557

A company is designing an application to run in a VPC on AWS. The application consists of Amazon EC2 instances that run in private subnets as part of an Auto Scaling group. The application also includes a Network Load Balancer that extends across public subnets. The application stores data in an Amazon RDS DB instance.

The company has attached a security group that is named "web-servers" to the EC2 instances. The company has attached a security group that is named "database" to the DB instance.

How should a solutions architect configure the communication between the EC2 instances and the DB instance?

A. Configure the "web-servers" security group to allow access to the DB instance's current IP addresses. Configure the "database" security group to allow access from the current set of IP addresses in use by the EC2 instances.

B. Configure the "web-servers" security group to allow access to the "database" security group. Configure the "database" security group to allow access from the "web-servers" security group.

C. Configure the "web-servers" security group to allow access to the DB instance's current IP addresses. Configure the "database" security group to allow access from the Auto Scaling group.

D. Configure the "web-servers" security group to allow access to the "database" security group. Configure the "database" security group to allow access from the Auto Scaling group.

Answer: C

Explanation:

Question: 558

A company wants an AWS Lambda function to call a third-party API and save the response to a private Amazon RDS DB instance in the same private subnet.

What should a solutions architect do to meet these requirements?

- A. Create a NAT gateway. In the route table for the private subnet, add a route to the NAT gateway. Attach the Lambda function to the private subnet. Create an IAM role that includes the AWSLambdaBasicExecutionRole permissions policy. Attach the role to the Lambda function.
- B. Create an internet gateway. In the route table for the private subnet, add a route to the internet gateway. Attach the Lambda function to the private subnet. Create an IAM role that includes the AWSLambdaBasicExecutionRole permissions policy. Attach the role to the Lambda function.
- C. Create a NAT gateway. In the route table for the private subnet, add a route to the NAT gateway. Attach the Lambda function to the private subnet. Create an IAM role that includes the AWSLambdaVPCAccessExecutionRole permissions policy. Attach the role to the Lambda function.
- D. Create an internet gateway. In the route table for the private subnet, add a route to the internet gateway. Attach the Lambda function to the private subnet. Create an IAM role that includes the AWSLambdaVPCAccessExecutionRole permissions policy. Attach the role to the Lambda function.

Answer: B

Explanation:

Question: 559

A company has a stateless asynchronous application that runs in an Apache Hadoop cluster. The application is invoked on demand to run extract, transform and load (ETL) jobs several times a day. A solutions architect needs to migrate this application to the AWS Cloud by designing an Amazon EMR cluster for the workload. The cluster must be available immediately to process jobs. Which implementation meets these requirements MOST cost-effectively?

- A. Use zonal Reserved Instances for the master nodes and the core nodes. Use a Spot Fleet for the task nodes.
- B. Use zonal Reserved Instances for the master nodes. Use Spot instances for the core nodes and the task nodes.
- C. Use regional Reserved Instances for the master nodes. Use a Spot Fleet for the core nodes and the task nodes.
- D. Use regional Reserved Instances for the master nodes. Use On-Demand Capacity Reservations for the core nodes and the task nodes.

Answer: A

Explanation:

Question: 560

A media company is using video conversion tools that run on Amazon EC2 instances. The video conversion tools run on a combination of Windows EC2 instances and Linux EC2 instances. Each video file is tens of gigabytes in size. The video conversion tools must process the video files in the shortest possible amount of time. The company needs a single, centralized file storage solution that can be mounted on all the EC2 instances that host the video conversion tools.

Which solution will meet these requirements?

- A. Deploy Amazon FSx for Windows File Server with hard disk drive (HDD) storage
- B. Deploy Amazon FSx for Windows File Server with solid state drive (SSD) storage
- C. Deploy Amazon Elastic File System (Amazon EFS) with Max I/O performance mode
- D. Deploy Amazon Elastic File System (Amazon EFS) with General Purpose performance mode

Answer: D

Explanation:

Question: 561

A company's order system sends requests from clients to Amazon EC2 instances. The EC2 instances process the orders and then store the orders in a database on Amazon RDS. Users report that they must reprocess orders when the system fails. The company wants a resilient solution that can process orders automatically if a system outage occurs.

What should a solutions architect do to meet these requirements?

- A. Move the EC2 instances into an Auto Scaling group. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to target an Amazon Elastic Container Service (Amazon ECS) task.
- B. Move the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB). Update the order system to send messages to the ALB endpoint.
- C. Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function, and subscribe the function to the SNS topic. Configure the order system to send messages to the SNS topic. Send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command.

Answer: C

Explanation:

Question: 562

A company has an application that processes customer orders. The company hosts the application on an Amazon EC2 instance that saves the orders to an Amazon Aurora database. Occasionally when traffic is high, the workload does not process orders fast enough.

What should a solutions architect do to write the orders reliably to the database as quickly as possible?

- A. Increase the instance size of the EC2 instance when traffic is high. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic.
- B. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.
- C. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database

endpoint to the SNS topic. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SNS topic.

D. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue when the EC2 instance reaches CPU threshold limits. Use scheduled scaling of EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database

Answer: B

Explanation:

Question: 563

A company runs a critical customer-facing application on Amazon Elastic Kubernetes Service (Amazon EKS). The application has a microservices architecture. The company needs to implement a solution that collects, aggregates and summarizes metrics and logs from the application in a centralized location.

Which solution meets these requirements?

- A. Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
- B. Run AWS App Mesh in the existing EKS cluster. View the metrics and logs in the App Mesh console.
- C. Configure AWS CloudTrail to capture data events. Query CloudTrail by using Amazon OpenSearch Service (Amazon Elasticsearch Service).
- D. Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console.

Answer: C

Explanation:

Question: 564

A company is deploying a new application to Amazon Elastic Kubernetes Service (Amazon EKS) with an AWS Fargate cluster. The application needs a storage solution for data persistence. The solution must be highly available and fault tolerant. The solution also must be shared between multiple application containers.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create Amazon Elastic Block Store (Amazon EBS) volumes in the same Availability Zones where EKS worker nodes are placed. Register the volumes in a StorageClass object on an EKS cluster. Use EBS Multi-Attach to share the data between containers.
- B. Create an Amazon Elastic File System (Amazon EFS) file system. Register the file system in a StorageClass object on an EKS cluster. Use the same file system for all containers.
- C. Create an Amazon Elastic Block Store (Amazon EBS) volume. Register the volume in a StorageClass object on an EKS cluster. Use the same volume for all containers.
- D. Create Amazon Elastic File System (Amazon EFS) file systems in the same Availability Zones where EKS worker nodes are placed. Register the file systems in a StorageClass object on an EKS cluster. Create an AWS Lambda function to synchronize the data between file systems.

Answer: B

Explanation:

Question: 565

A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.

Which combination of steps should a solutions architect take to accomplish this? (Select TWO.)

- A. Configure a VPC gateway endpoint (or Amazon S3 within the VPC)
- B. Create a bucket policy to make the objects in the S3 bucket public
- C. Create a bucket policy that limits access to only the application tier running in the VPC
- D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance
- E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket

Answer: BD

Explanation:

Question: 566

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Server-side encryption with customer-provided keys (SSE-C)
- B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
- C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation
- D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

Answer: D

Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>

When you enable automatic key rotation for a customer managed key, AWS KMS generates new cryptographic material for the KMS key every year. AWS KMS also saves the KMS key's older cryptographic material in perpetuity so it can be used to decrypt data that the KMS key encrypted.

Key rotation in AWS KMS is a cryptographic best practice that is designed to be transparent and easy to use. AWS KMS supports optional automatic key rotation only for customer managed CMKs. Enable and disable key rotation. Automatic key rotation is disabled by default on customer managed CMKs. When you enable (or re-enable) key rotation, AWS KMS automatically rotates the CMK 365 days after the enable date and every 365 days thereafter.

Question: 567

A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible.

Which solution will meet these requirements?

- A. Configure the Requester Pays feature on the company's S3 bucket.
- B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.
- C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.
- D. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

Answer: A

Explanation:

Question: 568

A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event.

A solutions architect needs to design a solution that stores customer data that is created during database upgrades.

Which solution will meet these requirements?

- A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.
- B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.
- C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.
- D. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Answer: C

Explanation:

Question: 569

A company has an application that loads documents into an Amazon S3 bucket and converts the

documents into another format. The application stores the converted documents in another S3 bucket and saves the document name and URLs in an Amazon DynamoDB table. The DynamoDB entries are used during subsequent days to access the documents. The company uses a DynamoDB Accelerator (DAX) cluster in front of the table.

Recently, traffic to the application has increased. Document processing tasks are timing out during the scheduled DAX maintenance window. A solutions architect must ensure that the documents continue to load during the maintenance window.

What should the solutions architect do to accomplish this goal?

- A. Modify the application to write to the DAX cluster. Configure the DAX cluster to write to the DynamoDB table when the maintenance window is complete.
- B. Enable Amazon DynamoDB Streams for the DynamoDB table. Modify the application to write to the stream. Configure the stream to load the data when the maintenance window is complete.
- C. Convert the application to an AWS Lambda function. Configure the Lambda function runtime to be longer than the maintenance window. Create an Amazon CloudWatch alarm to monitor Lambda timeouts.
- D. Modify the application to write the document name and URLs to an Amazon Simple Queue Service (Amazon SQS) queue. Create an AWS Lambda function to read the SQS queue and write to DynamoDB.

Answer: C

Explanation:

Question: 570

A company is creating a new application that will store a large amount of data.

a. The data will be analyzed hourly and will be modified by several Amazon EC2 Linux instances that are deployed across multiple Availability Zones. The needed amount of storage space will continue to grow for the next 6 months.

Which storage solution should a solutions architect recommend to meet these requirements?

- A. Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access to the application instances.
- B. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the application instances.
- C. Store the data in an Amazon Elastic File System (Amazon EFS) file system. Mount the file system on the application instances.
- D. Store the data in an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS volume shared between the application instances.

Answer: C

Explanation:

Question: 571

A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.

What should the solutions architect do to maximize reliability of the application infrastructure?

- A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.
- B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones
- C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.
- D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances. Update the DB instance to be Multi-AZ, and enable deletion protection.

Answer: B

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

Question: 572

A company has developed a new content-sharing application that runs on Amazon Elastic Container Service (Amazon ECS). The application runs on Amazon Linux Docker tasks that use the Amazon EC2 launch type. The application requires a storage solution that has the following characteristics:

- Accessibility (or multiple ECS tasks through bind mounts)
- Resiliency across Availability Zones
- Burstable throughput of up to 3 Gbps
- Ability to be scaled up over time

Which storage solution meets these requirements?

- A. Launch an Amazon FSx for Windows File Server Multi-AZ instance. Configure the ECS task definitions to mount the Amazon FSx instance volume at launch.
- B. Launch an Amazon Elastic File System (Amazon EFS) instance. Configure the ECS task definitions to mount the EFS Instance volume at launch.
- C. Create a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume with Multi-Attach set to enabled. Attach the EBS volume to the ECS EC2 instance. Configure ECS task definitions to mount the EBS instance volume at launch.
- D. Launch an EC2 instance with several Provisioned IOPS SSD (k>2) Amazon Elastic Block Store (Amazon EBS) volumes attached in a RAID 0 configuration. Configure the EC2 instance as an NFS storage server. Configure ECS task definitions to mount the volumes at launch.

Answer: B

Explanation:

Question: 573

A company has 150 TB of archived image data stored on-premises that needs to be moved to the

AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only.

What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

- A. Use AWS Snowmobile to ship the data to AWS.
- B. Order multiple AWS Snowball devices to ship the data to AWS.
- C. Enable Amazon S3 Transfer Acceleration and securely upload the data.
- D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data

Answer: B

Explanation:

eg. 6 hrs night
 $6 \text{ hrs} * 60 \text{ min/hr} = 360 \text{ min}$
 $360 \text{ min} * 60 \text{ sec/min} = 21600 \text{ sec}$

$100 \text{ Mbps} * 21600 \text{ s} = 2160000 \text{ Mb}$
 or 2160 Gb or 2.1 TB can only be done

So, for 150 TB, we can use 2 X Snowball Edge Storage Optimised devices.

Size of Snowball Edge Storage Optimised device = 80 TB
 Size of Snowball Edge Compute Optimised device = 40 TB
 Size of Snowcone = 8 TB
 Size of Snowmobile = 100 PB (1 PB = 1000 TB)

Q: How should I choose between Snowmobile and Snowball?

To migrate large datasets of 10PB or more in a single location, you should use Snowmobile. For datasets less than 10PB or distributed in multiple locations, you should use Snowball. In addition, you should evaluate the amount of available bandwidth in your network backbone. If you have a high speed backbone with hundreds of Gb/s of spare throughput, then you can use Snowmobile to migrate the large datasets all at once. If you have limited bandwidth on your backbone, you should consider using multiple Snowballs to migrate the data incrementally.

Question: 574

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored. Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon

Machine image (AMI) that consists of the processor application Create a launch configuration that uses the AMI Create an Auto Scaling group using the launch configuration Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage

C. Create an Amazon SQS queue to hold the jobs that needs to be processed Create an Amazon Machine image (AMI) that consists of the processor application Create a launch template that uses the AMI Create an Auto Scaling group using the launch template Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue

D. Create an Amazon SNS topic to send the jobs that need to be processed Create an Amazon Machine Image (AMI) that consists of the processor application Create a launch template that uses the AMI Create an Auto Scaling group using the launch template Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic

Answer: C

Explanation:

"Create an Amazon SQS queue to hold the jobs that needs to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue"

In this case we need to find a durable and loosely coupled solution for storing jobs. Amazon SQS is ideal for this use case and can be configured to use dynamic scaling based on the number of jobs waiting in the queue. To configure this scaling you can use the backlog per instance metric with the target value being the acceptable backlog per instance to maintain. You can calculate these numbers as follows: Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue

Question: 575

A company hosts its product information webpages on AWS The existing solution uses multiple Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website

What should a solutions architect do to meet these requirements?

- A. Redesign the application to use Amazon CloudFront
- B. Redesign the application to use AWS Elastic Beanstalk
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting

Answer: A

Explanation:

as CloudFront can help provide the best experience for global users. CloudFront integrates seamlessly with ALB and provides an option to use custom DNS and SSL certs.

Question: 576

A company's web application resizes uploaded images for users. The application stores the original images and the resized images in Amazon S3. The company needs to minimize the storage costs for all the images. Original images are viewed frequently, and resized images are viewed infrequently after they are created. Both types of images need to be immediately available. Which combination of actions should a solutions architect take to meet these requirements? (Select TWO.)

- A. Store the original images in S3 Standard.
- B. Store the resized images in S3 Standard.
- C. Store the original images in S3 Glacier.
- D. Store the resized images in S3 Glacier.
- E. Store the resized images in S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: AD

Explanation:

Question: 577

A company is developing an internal application that uses a PostgreSQL database. The company has decided to host the database on Amazon Aurora. The application does not need to be highly available, but data must be stored in multiple Availability Zones to maximize durability. Which database configuration meets these requirements MOST cost-effectively?

- A. An Aurora PostgreSQL DB cluster with a single DB instance.
- B. An Aurora PostgreSQL DB cluster with a primary DB instance and a read replica.
- C. An Aurora PostgreSQL DB cluster with Multi-AZ deployment enabled.
- D. An Aurora PostgreSQL global database cluster.

Answer: B

Explanation:

Question: 578

A company wants to experiment with individual AWS accounts for its engineering team. The company wants to be notified as soon as the Amazon EC2 instance usage for a given month exceeds a specific threshold for each account.

What should a solutions architect do to meet this requirement MOST cost-effectively?

- A. Use Cost Explorer to create a daily report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
- B. Use Cost Explorer to create a monthly report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.

- C. Use AWS Budgets to create a cost budget for each account Set the period to monthly Set the scope to EC2 instances Set an alert threshold for the budget Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.
- D. Use AWS Cost and Usage Reports to create a report with hourly granularity. Integrate the report data with Amazon Athena. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule an Athena query Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded

Answer: B

Explanation:

Question: 579

A company wants to run its critical applications in containers to meet requirements for scalability and availability The company prefers to focus on maintenance of the critical applications The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload

What should a solutions architect do to meet those requirements?

- A. Use Amazon EC2 Instances, and Install Docker on the Instances
- B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes
- C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate
- D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

Answer: C

Explanation:

using AWS ECS on AWS Fargate since they requirements are for scalability and availability without having to provision and manage the underlying infrastructure to run the containerized workload.

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html>

Question: 580

A company has chosen to rehost its application on Amazon EC2 instances The application occasionally experiences errors that affect parts of its functionality The company was unaware of this issue until users reported the errors The company wants to address this problem during the migration and reduce the time it takes to detect issues with the application Log files for the application are stored on the local disk.

A solutions architect needs to design a solution that will alert staff if there are errors in the application after the application is migrated to AWS. The solution must not require additional changes to the application code.

What is the MOST operationally efficient solution that meets these requirements?

- A. Configure the application to generate custom metrics for the errors Send these metric data points to Amazon CloudWatch by using the PutMetricData API call Create a CloudWatch alarm that is based

on the custom metrics

B. Create an hourly cron job on the instances to copy the application log data to an Amazon S3 bucket. Configure an AWS Lambda function to scan the log file and publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to alert staff if errors are detected.

C. Install the Amazon CloudWatch agent on the instances. Configure the CloudWatch agent to stream the application log file to Amazon CloudWatch Logs. Run a CloudWatch Logs insights query to search for the relevant pattern in the log file. Create a CloudWatch alarm that is based on the query output.

D. Install the Amazon CloudWatch agent on the instances. Configure the CloudWatch agent to stream the application log file to Amazon CloudWatch Logs. Create a metric filter for the relevant log group. Define the filter pattern that is required to determine that there are errors in the application. Create a CloudWatch alarm that is based on the resulting metric.

Answer: B

Explanation:

Question: 581

An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service: free and paid. Photos submitted by paid users are processed before those submitted by free users. Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS.

Which configuration should a solutions architect recommend?

A. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.

B. Use two SQS FIFO queues: one for paid and one for free. Set the free queue to use short polling and the paid queue to use long polling.

C. Use two SQS standard queues: one for paid and one for free. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.

D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero. Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first.

Answer: C

Explanation:

<https://acloud.guru/forums/guru-of-the-week/discussion/-L7Be8rOao3InQxdQcXj/>

<https://aws.amazon.com/sqs/features/>

Priority: Use separate queues to provide prioritization of work.

<https://aws.amazon.com/sqs/features/>

<https://aws.amazon.com/sqs/features/#:~:text=Priority%3A%20Use%20separate%20queues%20to%20provide%20prioritization%20of%20work.>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-short-and-long-polling.html>

Question: 582

A company is migrating a distributed application to AWS. The application serves variable workloads. The legacy platform consists of a primary server that coordinates jobs across multiple compute nodes. The company wants to modernize the application with a solution that maximizes resiliency and scalability.

How should a solutions architect design the architecture to meet these requirements?

- A. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling to use scheduled scaling.
- B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.
- C. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure AWS CloudTrail as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the primary server.
- D. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure Amazon EventBridge (Amazon CloudWatch Events) as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the compute nodes.

Answer: C

Explanation:

Question: 583

A company is implementing a shared storage solution for a media application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.

Which AWS solution meets these requirements?

- A. Create an AWS Storage Gateway volume gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- B. Create an AWS Storage Gateway tape gateway. Configure it to use Amazon S3. Connect the application server to the tape gateway.
- C. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- D. Create an Amazon FSx for Windows File System. Attach the file system to the origin server. Connect the application server to the file system.

Answer: D

Explanation:

Question: 584

A company is experiencing sudden increases in demand. The company needs to provision large Amazon EC2 instances from an Amazon Machine Image (AMI). The instances will run in an Auto Scaling group. The company needs a solution that provides minimum initialization latency to meet the demand.

Which solution meets these requirements?

- A. Use the `aws ec2 register-image` command to create an AMI from a snapshot Use AWS Step Functions to replace the AMI in the Auto Scaling group
- B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot Provision an AMI by using the snapshot Replace the AMI in the Auto Scaling group with the new AMI
- C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM) Create an AWS Lambda function that modifies the AMI in the Auto Scaling group
- D. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke AWS Backup lifecycle policies that provision AMIs Configure Auto Scaling group capacity limits as an event source in EventBridge (CloudWatch Events)

Answer: B

Explanation:

Question: 585

A company uses Amazon EC2 instances to host its internal systems As part of a deployment operation, an administrator tries to use the AWS CLI to terminate an EC2 instance However, the administrator receives a 403 (Access Denied) error message The administrator is using an IAM role that has the following IAM policy attached:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["ec2:TerminateInstances"],
      "Resource": ["*"]
    },
    {
      "Effect": "Deny",
      "Action": ["ec2:TerminateInstances"],
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ],
  "Resource": ["*"]
}
```

What is the cause of the unsuccessful request?

- A. The EC2 Instance has a resource-based policy with a Deny statement.
- B. The principal has not been specified in the policy statement
- C. The "Action" field does not grant the actions that are required to terminate the EC2 instance
- D. The request to terminate the EC2 instance does not originate from the CIDR blocks 192.0.2.0/24 or 203.0.113.0/24.

Answer: B

Explanation:

Question: 586

A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.

What should the solutions architect do to meet these requirements?

- A. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.
- B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
- C. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
- D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Answer: A

Explanation:

Question: 587

A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years. The log files will be analyzed by a reporting tool that must be able to access all the files concurrently.

Which storage solution meets these requirements MOST cost-effectively?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon EC2 instance store
- D. Amazon S3

Answer: D

Explanation:

Thank You for your purchase
Amazon SAA-C02 Exam Question & Answers
AWS Certified Solutions Architect - Associate Exam
Exam