



AWS CERTIFIED SOLUTIONS ARCHITECT ASSOCIATE

**Test your AWS knowledge with
exam-difficulty practice questions
for offline study**

Neal Davis

 DigitalCloud
TRAINING

GETTING STARTED

WELCOME

Congratulations on choosing to embark on your journey to become a Solutions Architect! You have just gained access to the highest quality practice tests for the AWS Solutions Architect Associate certification exam. These practice tests will prepare you thoroughly for the real exam so that you pass with flying colors.

There are **6 practice exams with 65 questions** each and each set of practice exams includes questions from the four domains of the latest **SAA-C03** exam. All **390 practice questions** were designed to reflect the difficulty of the real AWS exam. With these Practice Tests, you'll know when you are ready to pass your AWS Solutions Architect Associate exam the first time! We recommend re-taking these practice tests until you consistently score 80% or higher - that's when you're ready to sit the exam and achieve a great score!

If you want easy to pass questions, then these Practice Tests are not for you! Our students love these high-quality practice tests because they **match the level of difficulty and exam pattern** of the actual certification exam and help them understand the AWS concepts. Students who have recently passed the SAA-C03 exam confirm that these AWS practice questions are the most similar to the real exam.

I hope you get great value from this resource that has been well received by our pool of over 750,000 students. Through diligent study of these questions, you will be in the perfect position to ace your AWS Certified Solutions Architect Associate exam with confidence.

Wishing you the best for every step in your cloud journey!

Neal Davis

Neal Davis
Founder of Digital Cloud Training



WHAT DO OTHER STUDENTS SAY?

Check out the excellent reviews from our many students who passed their AWS exam with an average passing score of over 850:

* * * * *

The questions in this study guide are as real as they can get. Tricky to answer correctly unless you know AWS well and have some real experience of the system. Just like the real exam.

* * * * *

Neal has put together a great set of questions that progressively get more difficult. I find this method very appealing and easy to learn. Passed my exam on the first try. These books are a must buy if you're serious about becoming a certified architect.

* * * * *

These questions were very helpful in studying for the exam. I liked that the questions gave references to the online AWS documentation so you can study the subject if necessary.

* * * * *

I just passed my exam. This practice exams and explanations were key to understand the exam logic and type of questions the real exam has.

* * * * *

These questions are in the same format and around the same degree of difficulty with the real exam. It's super helpful to prepare for the exam and pass with confidence. Highly recommended.

HOW TO BEST USE THIS RESOURCE

We have organized the 390 practice questions into 6 sets and each set is repeated once without answers and explanations and once with answers and explanations. This allows you to choose from two methods of preparation.

1. Exam simulation

To simulate the exam experience, use the “PRACTICE QUESTIONS ONLY” sets. Grab a pen and paper to record your answers for all 65 questions. After completing each set, check your answers using the “PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS” section.

To calculate your total score, sum up the number of correct answers and multiply them by 1.54 (weighting out of 100%) to get your percentage score out of 100%. For example, if you got 50 questions right, the calculation would be $50 \times 1.54 = 77\%$. The pass mark of the official AWS exam is 72%.

2. Training mode

To use the practice questions as a learning tool, use the “PRACTICE QUESTIONS, ANSWERS & EXPLANATIONS” sets to view the answers and read the in-depth explanations as you move through the questions.

KEY TRAINING ADVICE

AIM FOR A MINIMUM SCORE OF 80%: Although the actual AWS exam has a pass mark of 72%, we recommend that you repeatedly retake our AWS practice exams until you consistently score 80% or higher. We encourage you to put in the work and study the explanations in detail. Once you achieve the recommended score in the practice tests - you are ready to sit the exam and achieve a great score!

FAMILIARIZE YOURSELF WITH THE QUESTION STYLE: Using our AWS practice exams helps you gain experience with the test question format and exam approach for the latest SAA-C03 exam. You'll become intimately familiar with how the questions in the real AWS exam are structured and will be adequately prepared for the real AWS exam experience.

DEEPEN YOUR KNOWLEDGE: Please note that though we match the AWS exam pattern, our AWS practice exams are NOT brain dumps. Don't expect to pass the real AWS certification exam by simply memorizing answers. Instead, we encourage you to use these practice tests to deepen your knowledge. This is your best chance to successfully pass your exam - no matter what questions you are presented with.

YOUR PATHWAY TO SUCCESS

- Enroll in Instructor-led Video Course**
Familiarize yourself with the AWS platform
- Take our AWS Practice Exams**
Identify your strengths and weaknesses and assess your exam readiness
- Study Training Notes**
Focus your study on the knowledge areas where you need to most
- Get AWS Certified**
This pathway will let you pass your AWS exam first time with confidence



Instructor-led Video Course

To get you started, we'd suggest first enrolling in the on-demand AWS Certified Solutions Architect Associate video course from Digital Cloud Training to familiarize yourself with the AWS platform before assessing your exam readiness with these practice exams.

Training Notes

Use the Training Notes for the AWS Certified Solutions Architect Associate from Digital Cloud Training to get a more detailed understanding of the AWS services and focus your study on the knowledge areas where you need to most. Deep dive into the SAA-C03 exam objectives with detailed facts, tables and diagrams to shortcut your time to success.

To learn more about our AWS training, visit <https://digitalcloud.training/aws-certified-solutions-architect-associate/>

CONTACT, FEEDBACK & SHARING

We want you to get great value from these training resources. If for any reason you are not 100% satisfied, please contact us at support@digitalcloud.training. We promise to address all questions and concerns, typically within 24hrs. We really want you to have a 5-star learning experience!

The AWS platform is evolving quickly, and the exam tracks these changes with a typical lag of around 6 months. We are therefore reliant on student feedback to keep track of what is appearing in the exam. If there are any topics in your exam that weren't covered in our training resources, please provide us with feedback using this form <https://digitalcloud.training/student-feedback/>. We appreciate any feedback that will help us further improve our AWS training resources.

CONNECT WITH US ON SOCIAL MEDIA

To learn about the different ways of connecting with us, visit: <https://digitalcloud.training/about-neal-davis-and-digital-cloud-training/>



digitalcloud.training



facebook.com/digitalcloudtraining



linkedin.com/company/digitalcloudtraining



youtube.com/c/digitalcloudtraining



Twitter @[digitalcloudt](https://twitter.com/digitalcloudt)



Instagram @[digitalcloudtraining](https://instagram.com/digitalcloudtraining)

TABLE OF CONTENTS

GETTING STARTED	2
Welcome	2
What do other Students say?.....	2
How to Best Use This Resource	3
Key Training Advice	3
Your Pathway to Success.....	3
Contact, Feedback & Sharing	4
Connect with us on Social Media	4
SET 1: PRACTICE QUESTIONS ONLY	6
SET 1: PRACTICE QUESTIONS AND ANSWERS	21
SET 2: PRACTICE QUESTIONS ONLY	72
SET 2: PRACTICE QUESTIONS AND ANSWERS	86
SET 3: PRACTICE QUESTIONS ONLY	141
SET 3: PRACTICE QUESTIONS AND ANSWERS	157
SET 4: PRACTICE QUESTIONS ONLY	212
SET 4: PRACTICE QUESTIONS AND ANSWERS	225
SET 5: PRACTICE QUESTIONS ONLY	270
SET 5: PRACTICE QUESTIONS AND ANSWERS	283
SET 6: PRACTICE QUESTIONS ONLY	326
SET 6: PRACTICE QUESTIONS AND ANSWERS	339
CONCLUSION	383
Reach Out and Connect.....	383
LIVE BOOTCAMPS, ON-DEMAND TRAINING AND CHALLENGE LABS.....	384
ABOUT THE AUTHOR	385

SET 1: PRACTICE QUESTIONS ONLY

For training purposes, go directly to [Set 1: Practice Questions, Answers & Explanations](#)

QUESTION 1

A company has two accounts for perform testing and each account has a single VPC: VPC-TEST1 and VPC-TEST2. The operations team require a method of securely copying files between Amazon EC2 instances in these VPCs. The connectivity should not have any single points of failure or bandwidth constraints.

Which solution should a Solutions Architect recommend?

1. Create a VPC gateway endpoint for each EC2 instance and update route tables.
2. Attach a virtual private gateway to VPC-TEST1 and VPC-TEST2 and enable routing.
3. Attach a Direct Connect gateway to VPC-TEST1 and VPC-TEST2 and enable routing.
4. Create a VPC peering connection between VPC-TEST1 and VPC-TEST2.

QUESTION 2

A Solutions Architect has deployed an application on several Amazon EC2 instances across three private subnets. The application must be made accessible to internet-based clients with the least amount of administrative effort.

How can the Solutions Architect make the application available on the internet?

1. Create an Amazon Machine Image (AMI) of the instances in the private subnet and launch new instances from the AMI in public subnets. Create an Application Load Balancer and add the public instances to the ALB.
2. Create an Application Load Balancer and associate three public subnets from the same Availability Zones as the private instances. Add the private instances to the ALB.
3. Create an Application Load Balancer and associate three private subnets from the same Availability Zones as the private instances. Add the private instances to the ALB.
4. Create a NAT gateway in a public subnet. Add a route to the NAT gateway to the route tables of the three private subnets.

QUESTION 3

A video production company is planning to move some of its workloads to the AWS Cloud. The company will require around 5 TB of storage for video processing with the maximum possible I/O performance. They also require over 400 TB of extremely durable storage for storing video files and 800 TB of storage for long-term archival.

Which combinations of services should a Solutions Architect use to meet these requirements?

1. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage.
2. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage.
3. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage.
4. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage.

QUESTION 4

A company provides a REST-based interface to an application that allows a partner company to send data in near-real time. The application then processes the data that is received and stores it for later analysis. The application runs on Amazon EC2 instances.

The partner company has received many 503 Service Unavailable Errors when sending data to the application and the compute capacity reaches its limits and is unable to process requests when spikes in data volume occur.

Which design should a Solutions Architect implement to improve scalability?

1. Use Amazon API Gateway in front of the existing application. Create a usage plan with a quota limit for the partner company.

2. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
3. Use Amazon SQS to ingest the data. Configure the EC2 instances to process messages from the SQS queue.
4. Use Amazon SNS to ingest the data and trigger AWS Lambda functions to process the data in near-real time.

QUESTION 5

A persistent database must be migrated from an on-premises server to an Amazon EC2 instances. The database requires 64,000 IOPS and, if possible, should be stored on a single Amazon EBS volume.

Which solution should a Solutions Architect recommend?

1. Use an instance from the I3 I/O optimized family and leverage instance store storage to achieve the IOPS requirement.
2. Create an Amazon EC2 instance with four Amazon EBS General Purpose SSD (gp2) volumes attached. Max out the IOPS on each volume and use a RAID 0 stripe set.
3. Create a Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Provision 64,000 IOPS for the volume.
4. Create an Amazon EC2 instance with two Amazon EBS Provisioned IOPS SSD (io1) volumes attached. Provision 32,000 IOPS per volume and create a logical volume using the OS that aggregates the capacity.

QUESTION 6

A company uses an Amazon RDS MySQL database instance to store customer order data. The security team have requested that SSL/TLS encryption in transit must be used for encrypting connections to the database from application servers. The data in the database is currently encrypted at rest using an AWS KMS key.

How can a Solutions Architect enable encryption in transit?

1. Enable encryption in transit using the RDS Management console and obtain a key using AWS KMS.
2. Add a self-signed certificate to the RDS DB instance. Use the certificates in all connections to the RDS DB instance.
3. Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption in transit enabled.
4. Download the AWS-provided root certificates. Use the certificates when connecting to the RDS DB instance.

QUESTION 7

An eCommerce company runs an application on Amazon EC2 instances in public and private subnets. The web application runs in a public subnet and the database runs in a private subnet. Both the public and private subnets are in a single Availability Zone.

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

1. Create new public and private subnets in the same AZ but in a different Amazon VPC.
2. Create an EC2 Auto Scaling group in the public subnet and use an Application Load Balancer.
3. Create an EC2 Auto Scaling group and Application Load Balancer that spans across multiple AZs.
4. Create new public and private subnets in a different AZ. Create a database using Amazon EC2 in one AZ.
5. Create new public and private subnets in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment.

QUESTION 8

A company runs an application on six web application servers in an Amazon EC2 Auto Scaling group in a single Availability Zone. The application is fronted by an Application Load Balancer (ALB). A Solutions Architect needs to modify the infrastructure to be highly available without making any modifications to the application.

Which architecture should the Solutions Architect choose to enable high availability?

1. Create an Amazon CloudFront distribution with a custom origin across multiple Regions.
2. Modify the Auto Scaling group to use two instances across each of three Availability Zones.
3. Create a launch template that can be used to quickly create more instances in another Region.
4. Create an Auto Scaling group to launch three instances across each of two Regions.

QUESTION 9

A web application allows users to upload photos and add graphical elements to them. The application offers two tiers of

service: free and paid. Photos uploaded by paid users should be processed before those submitted using the free tier. The photos are uploaded to an Amazon S3 bucket which uses an event notification to send the job information to Amazon SQS.

How should a Solutions Architect configure the Amazon SQS deployment to meet these requirements?

1. Use one SQS standard queue. Use batching for the paid photos and short polling for the free photos.
2. Use a separate SQS FIFO queue for each tier. Set the free queue to use short polling and the paid queue to use long polling.
3. Use a separate SQS Standard queue for each tier. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.
4. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.

QUESTION 10

A company has deployed a new website on Amazon EC2 instances behind an Application Load Balancer (ALB). Amazon Route 53 is used for the DNS service. The company has asked a Solutions Architect to create a backup website with support contact details that users will be directed to automatically if the primary website is down.

How should the Solutions Architect deploy this solution cost-effectively?

1. Configure a static website using Amazon S3 and create a Route 53 weighted routing policy.
2. Deploy the backup website on EC2 and ALB in another Region and use Route 53 health checks for failover routing.
3. Create the backup website on EC2 and ALB in another Region and create an AWS Global Accelerator endpoint.
4. Configure a static website using Amazon S3 and create a Route 53 failover routing policy.

QUESTION 11

A company requires that all AWS IAM user accounts have specific complexity requirements and minimum password length.

How should a Solutions Architect accomplish this?

1. Set a password policy for each IAM user in the AWS account.
2. Set a password policy for the entire AWS account.
3. Create an IAM policy that enforces the requirements and apply it to all users.
4. Use an AWS Config rule to enforce the requirements when creating user accounts.

QUESTION 12

A company runs a dynamic website that is hosted on an on-premises server in the United States. The company is expanding to Europe and is investigating how they can optimize the performance of the website for European users. The website's backed must remain in the United States. The company requires a solution that can be implemented within a few days.

What should a Solutions Architect recommend?

1. Use Amazon CloudFront with Lambda@Edge to direct traffic to an on-premises origin.
2. Launch an Amazon EC2 instance in an AWS Region in the United States and migrate the website to it.
3. Migrate the website to Amazon S3. Use cross-Region replication between Regions and a latency-based Route 53 policy.
4. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

QUESTION 13

A company runs an application in an on-premises data center that collects environmental data from production machinery. The data consists of JSON files stored on network attached storage (NAS) and around 5 TB of data is collected each day. The company must upload this data to Amazon S3 where it can be processed by an analytics application. The data must be transferred securely.

Which solution offers the MOST reliable and time-efficient data transfer?

1. AWS Database Migration Service over the Internet.
2. Amazon S3 Transfer Acceleration over the Internet.
3. AWS DataSync over AWS Direct Connect.
4. Multiple AWS Snowcone devices.

QUESTION 14

A company runs an application on an Amazon EC2 instance that requires 250 GB of storage space. The application is not used often and has small spikes in usage on weekday mornings and afternoons. The disk I/O can vary with peaks hitting a maximum of 3,000 IOPS. A Solutions Architect must recommend the most cost-effective storage solution that delivers the performance required.

Which configuration should the Solutions Architect recommend?

Which solution should the solutions architect recommend?

1. Amazon EBS Cold HDD (sc1)
2. Amazon EBS General Purpose SSD (gp2)
3. Amazon EBS Provisioned IOPS SSD (io1)
4. Amazon EBS Throughput Optimized HDD (st1)

QUESTION 15

A company offers an online product brochure that is delivered from a static website running on Amazon S3. The company's customers are mainly in the United States, Canada, and Europe. The company is looking to cost-effectively reduce the latency for users in these regions.

What is the most cost-effective solution to these requirements?

1. Create an Amazon CloudFront distribution that uses origins in U.S, Canada and Europe.
2. Create an Amazon CloudFront distribution and use Lambda@Edge to run the website's data processing closer to the users.
3. Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Europe.
4. Create an Amazon CloudFront distribution and set the price class to use all Edge Locations for best performance.

QUESTION 16

A developer created an application that uses Amazon EC2 and an Amazon RDS MySQL database instance. The developer stored the database user name and password in a configuration file on the root EBS volume of the EC2 application instance. A Solutions Architect has been asked to design a more secure solution.

What should the Solutions Architect do to achieve this requirement?

1. Move the configuration file to an Amazon S3 bucket. Create an IAM role with permission to the bucket and attach it to the EC2 instance.
2. Attach an additional volume to the EC2 instance with encryption enabled. Move the configuration file to the encrypted volume.
3. Install an Amazon-trusted root certificate on the application instance and use SSL/TLS encrypted connections to the database.
4. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.

QUESTION 17

A financial services company has a web application with an application tier running in the U.S and Europe. The database tier consists of a MySQL database running on Amazon EC2 in us-west-1. Users are directed to the closest application tier using Route 53 latency-based routing. The users in Europe have reported poor performance when running queries.

Which changes should a Solutions Architect make to the database tier to improve performance?

1. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
2. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure the application tier in Europe to use the local reader endpoint.
3. Migrate the database to Amazon RedShift. Use AWS DMS to synchronize data. Configure applications to use the RedShift data warehouse for queries.
4. Create an Amazon RDS Read Replica in one of the European regions. Configure the application tier in Europe to use the read replica for queries.

QUESTION 18

A company runs an application that uses an Amazon RDS PostgreSQL database. The database is currently not encrypted. A Solutions Architect has been instructed that due to new compliance requirements all existing and new data in the database must be encrypted. The database experiences high volumes of changes and no data can be lost.

How can the Solutions Architect enable encryption for the database without incurring any data loss?

1. Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot. Configure the application to use the new DB endpoint.
2. Create an RDS read replica and specify an encryption key. Promote the encrypted read replica to primary. Update the application to point to the new RDS DB endpoint.
3. Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs.
4. Update the RDS DB to Multi-AZ mode and enable encryption for the standby replica. Perform a failover to the standby instance and then delete the unencrypted RDS DB instance.

QUESTION 19

A company runs an application in a factory that has a small rack of physical compute resources. The application stores data on a network attached storage (NAS) device using the NFS protocol. The company requires a daily offsite backup of the application data.

Which solution can a Solutions Architect recommend to meet this requirement?

1. Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
2. Use an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
3. Use an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.
4. Create an IPSec VPN to AWS and configure the application to mount the Amazon EFS file system. Run a copy job to backup the data to EFS.

QUESTION 20

A company is deploying a fleet of Amazon EC2 instances running Linux across multiple Availability Zones within an AWS Region. The application requires a data storage solution that can be accessed by all of the EC2 instances simultaneously. The solution must be highly scalable and easy to implement. The storage must be mounted using the NFS protocol.

Which solution meets these requirements?

1. Create an Amazon S3 bucket and create an S3 gateway endpoint to allow access to the file system using the NFS protocol.
2. Create an Amazon EFS file system with mount targets in each Availability Zone. Configure the application instances to mount the file system.
3. Create an Amazon EBS volume and use EBS Multi-Attach to mount the volume to all EC2 instances across each Availability Zone.
4. Create an Amazon RDS database and store the data in a BLOB format. Point the application instances to the RDS endpoint.

QUESTION 21

A company is working with a strategic partner that has an application that must be able to send messages to one of the company's Amazon SQS queues. The partner company has its own AWS account.

How can a Solutions Architect provide least privilege access to the partner?

1. Create a user account that and grant the sqs:SendMessage permission for Amazon SQS. Share the credentials with the partner company.
2. Create a cross-account role with access to all SQS queues and use the partner's AWS account in the trust document for the role.
3. Update the permission policy on the SQS queue to grant all permissions to the partner's AWS account.
4. Update the permission policy on the SQS queue to grant the sqs:SendMessage permission to the partner's AWS account.

QUESTION 22

A company is investigating methods to reduce the expenses associated with on-premises backup infrastructure. The Solutions Architect wants to reduce costs by eliminating the use of physical backup tapes. It is a requirement that existing backup applications and workflows should continue to function.

What should the Solutions Architect recommend?

1. Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL).
2. Create an Amazon EFS file system and connect the backup applications using the NFS protocol.
3. Create an Amazon EFS file system and connect the backup applications using the iSCSI protocol.
4. Connect the backup applications to an AWS Storage Gateway using the iSCSI protocol.

QUESTION 23

A Solutions Architect has been tasked with re-deploying an application running on AWS to enable high availability. The application processes messages that are received in an ActiveMQ queue running on a single Amazon EC2 instance. Messages are then processed by a consumer application running on Amazon EC2. After processing the messages the consumer application writes results to a MySQL database running on Amazon EC2.

Which architecture offers the highest availability and low operational complexity?

1. Deploy a second Active MQ server to another Availability Zone. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone.
2. Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone.
3. Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.
4. Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Create an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use an Amazon RDS MySQL database with Multi-AZ enabled.

QUESTION 24

Storage capacity has become an issue for a company that runs application servers on-premises. The servers are connected to a combination of block storage and NFS storage solutions. The company requires a solution that supports local caching without re-architecting its existing applications.

Which combination of changes can the company make to meet these requirements? (Select TWO.)

1. Use an AWS Storage Gateway file gateway to replace the NFS storage.
2. Use the mount command on servers to mount Amazon S3 buckets using NFS.
3. Use AWS Direct Connect and mount an Amazon FSx for Windows File Server using iSCSI.
4. Use an AWS Storage Gateway volume gateway to replace the block storage.
5. Use Amazon Elastic File System (EFS) volumes to replace the block storage.

QUESTION 25

A company hosts an application on Amazon EC2 instances behind Application Load Balancers in several AWS Regions. Distribution rights for the content require that users in different geographies must be served content from specific regions.

Which configuration meets these requirements?

1. Create Amazon Route 53 records with a geolocation routing policy.
2. Create Amazon Route 53 records with a geoproximity routing policy.
3. Configure Amazon CloudFront with multiple origins and AWS WAF.
4. Configure Application Load Balancers with multi-Region routing.

QUESTION 26

A company plans to make an Amazon EC2 Linux instance unavailable outside of business hours to save costs. The instance is backed by an Amazon EBS volume. There is a requirement that the contents of the instance's memory must be preserved when it is made unavailable.

How can a solutions architect meet these requirements?

1. Stop the instance outside business hours. Start the instance again when required.
2. Hibernate the instance outside business hours. Start the instance again when required.
3. Use Auto Scaling to scale down the instance outside of business hours. Scale up the instance when required.
4. Terminate the instance outside business hours. Recover the instance again when required.

QUESTION 27

A Microsoft Windows file server farm uses Distributed File System Replication (DFSR) to synchronize data in an on-premises environment. The infrastructure is being migrated to the AWS Cloud.

Which service should the solutions architect use to replace the file server farm?

1. Amazon EFS
2. Amazon EBS
3. AWS Storage Gateway
4. Amazon FSx

QUESTION 28

An eCommerce application consists of three tiers. The web tier includes EC2 instances behind an Application Load balancer, the middle tier uses EC2 instances and an Amazon SQS queue to process orders, and the database tier consists of an Auto Scaling DynamoDB table. During busy periods customers have complained about delays in the processing of orders. A Solutions Architect has been tasked with reducing processing times.

Which action will be MOST effective in accomplishing this requirement?

1. Replace the Amazon SQS queue with Amazon Kinesis Data Firehose.
2. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.
3. Use Amazon DynamoDB Accelerator (DAX) in front of the DynamoDB backend tier.
4. Add an Amazon CloudFront distribution with a custom origin to cache the responses for the web tier.

QUESTION 29

A company uses Docker containers for many application workloads in an on-premise data center. The company is planning to deploy containers to AWS and the chief architect has mandated that the same configuration and administrative tools must be used across all containerized environments. The company also wishes to remain cloud agnostic to safeguard mitigate the impact of future changes in cloud strategy.

How can a Solutions Architect design a managed solution that will align with open-source software?

1. Launch the containers on Amazon Elastic Kubernetes Service (EKS) and EKS worker nodes.
2. Launch the containers on a fleet of Amazon EC2 instances in a cluster placement group.
3. Launch the containers on Amazon Elastic Container Service (ECS) with AWS Fargate instances.
4. Launch the containers on Amazon Elastic Container Service (ECS) with Amazon EC2 instance worker nodes.

QUESTION 30

A company has uploaded some highly critical data to an Amazon S3 bucket. Management are concerned about data availability and require that steps are taken to protect the data from accidental deletion. The data should still be accessible, and a user should be able to delete the data intentionally.

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

1. Enable versioning on the S3 bucket.
2. Enable MFA Delete on the S3 bucket.
3. Create a bucket policy on the S3 bucket.
4. Enable default encryption on the S3 bucket.
5. Create a lifecycle policy for the objects in the S3 bucket.

QUESTION 31

A company runs a large batch processing job at the end of every quarter. The processing job runs for 5 days and uses 15

Amazon EC2 instances. The processing must run uninterrupted for 5 hours per day. The company is investigating ways to reduce the cost of the batch processing job.

Which pricing model should the company choose?

1. Reserved Instances
2. Spot Instances
3. On-Demand Instances
4. Dedicated Instances

QUESTION 32

An application is being created that will use Amazon EC2 instances to generate and store data. Another set of EC2 instances will then analyze and modify the data. Storage requirements will be significant and will continue to grow over time. The application architects require a storage solution.

Which actions would meet these needs?

1. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances
2. Store the data in an Amazon EFS filesystem. Mount the file system on the application instances
3. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances
4. Store the data in AWS Storage Gateway. Setup AWS Direct Connect between the Gateway appliance and the EC2 instances

QUESTION 33

A company hosts a multiplayer game on AWS. The application uses Amazon EC2 instances in a single Availability Zone and users connect over Layer 4. Solutions Architect has been tasked with making the architecture highly available and also more cost-effective.

How can the solutions architect best meet these requirements? (Select TWO.)

1. Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically
2. Increase the number of instances and use smaller EC2 instance types
3. Configure a Network Load Balancer in front of the EC2 instances
4. Configure an Application Load Balancer in front of the EC2 instances
5. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically

QUESTION 34

A company delivers content to subscribers distributed globally from an application running on AWS. The application uses a fleet of Amazon EC2 instance in a private subnet behind an Application Load Balancer (ALB). Due to an update in copyright restrictions, it is necessary to block access for specific countries.

What is the EASIEST method to meet this requirement?

1. Modify the ALB security group to deny incoming traffic from blocked countries
2. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
3. Use Amazon CloudFront to serve the application and deny access to blocked countries
4. Use a network ACL to block the IP address ranges associated with the specific countries

QUESTION 35

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

1. Amazon EFS
2. Amazon FSx
3. Amazon S3
4. AWS Storage Gateway

QUESTION 36

A website runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) which serves as an origin for an Amazon CloudFront distribution. An AWS WAF is being used to protect against SQL injection attacks. A 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?

1. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address
2. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address
3. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address
4. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

QUESTION 37

A solutions architect is creating a system that will run analytics on financial data for several hours a night, 5 days a week. The analysis is expected to run for the same duration and cannot be interrupted once it is started. The system will be required for a minimum of 1 year.

What should the solutions architect configure to ensure the EC2 instances are available when they are needed?

1. Savings Plans
2. On-Demand Instances
3. Regional Reserved Instances
4. On-Demand Capacity Reservations

QUESTION 38

A solutions architect needs to backup some application log files from an online ecommerce store to Amazon S3. It is unknown how often the logs will be accessed or which logs will be accessed the most. The solutions architect must keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

1. S3 Glacier
2. S3 Intelligent-Tiering
3. S3 Standard-Infrequent Access (S3 Standard-IA)
4. S3 One Zone-Infrequent Access (S3 One Zone-IA)

QUESTION 39

A solutions architect is designing a new service that will use an Amazon API Gateway API on the frontend. The service will need to persist data in a backend database using key-value requests. Initially, the data requirements will be around 1 GB and future growth is unknown. Requests can range from 0 to over 800 requests per second.

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

1. AWS Fargate
2. AWS Lambda
3. Amazon DynamoDB
4. Amazon EC2 Auto Scaling
5. Amazon RDS

QUESTION 40

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.)

1. Detach a volume on an EC2 instance and copy it to an Amazon S3 bucket in the second Region
2. Launch a new EC2 instance from an Amazon Machine Image (AMI) in the second Region
3. Launch a new EC2 instance in the second Region and copy a volume from Amazon S3 to the new instance
4. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify the second Region for the destination

5. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the second Region using that EBS volume

QUESTION 41

A solutions architect is creating a document submission application for a school. The application will use 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 upload and modify the documents.

Which combination of actions should be taken to meet these requirements? (Select TWO.)

1. Set read-only permissions on the bucket
2. Enable versioning on the bucket
3. Attach an IAM policy to the bucket
4. Enable MFA Delete on the bucket
5. Encrypt the bucket using AWS SSE-S3

QUESTION 42

A solutions architect is designing an application on AWS. The compute layer will run in parallel across EC2 instances. The compute layer should scale based on the number of jobs to be processed. The compute layer 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?

1. Create an Amazon SNS topic to send the jobs that need 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 CPU usage
2. Create an Amazon SQS queue to hold the jobs that need 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 network usage
3. 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
4. Create an Amazon SNS topic to send the jobs that need 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 messages published to the SNS topic

QUESTION 43

A team are planning to run analytics jobs on log files each day and require a storage solution. The size and number of logs is unknown and data will persist for 24 hours only.

What is the MOST cost-effective solution?

1. Amazon S3 Glacier Deep Archive
2. Amazon S3 Standard
3. Amazon S3 Intelligent-Tiering
4. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

QUESTION 44

A company runs a web application that serves weather updates. The application runs on a fleet of Amazon EC2 instances in a Multi-AZ Auto scaling group behind an Application Load Balancer (ALB). The instances store data in an Amazon Aurora database. A solutions architect needs to make the application more resilient to sporadic increases in request rates.

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

1. Add and AWS WAF in front of the ALB
2. Add Amazon Aurora Replicas
3. Add an AWS Transit Gateway to the Availability Zones
4. Add an AWS Global Accelerator endpoint
5. Add an Amazon CloudFront distribution in front of the ALB

QUESTION 45

An Amazon VPC contains several Amazon EC2 instances. The instances need to make API calls to Amazon DynamoDB. A solutions architect needs to ensure that the API calls do not traverse the internet.

How can this be accomplished? (Select TWO.)

1. Create a route table entry for the endpoint
2. Create a gateway endpoint for DynamoDB
3. Create a new DynamoDB table that uses the endpoint
4. Create an ENI for the endpoint in each of the subnets of the VPC
5. Create a VPC peering connection between the VPC and DynamoDB

QUESTION 46

A solutions architect is designing the infrastructure to run an application on Amazon EC2 instances. The application requires high availability and must dynamically scale based on demand to be cost efficient.

What should the solutions architect do to meet these requirements?

1. Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Regions
2. Configure an Amazon CloudFront distribution in front of an Auto Scaling group to deploy instances to multiple Regions
3. Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Availability Zones
4. Configure an Amazon API Gateway API in front of an Auto Scaling group to deploy instances to multiple Availability Zones

QUESTION 47

A retail company with many stores and warehouses is implementing IoT sensors to gather monitoring data from devices in each location. The data will be sent to AWS in real time. A solutions architect must provide a solution for ensuring events are received in order for each device and ensure that data is saved for future processing.

Which solution would be MOST efficient?

1. Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3
2. Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS
3. Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS
4. Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3

QUESTION 48

An organization want to share regular updates about their charitable work using static webpages. The pages are expected to generate a large amount of views from 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?

1. Generate presigned URLs for the files
2. Use cross-Region replication to all Regions
3. Use the geoproximity feature of Amazon Route 53
4. Use Amazon CloudFront with the S3 bucket as its origin

QUESTION 49

An insurance company has a web application that serves users in the United Kingdom and Australia. The application includes a database tier using a MySQL database hosted in eu-west-2. The web tier runs from eu-west-2 and ap-southeast-2. Amazon Route 53 geoproximity routing is used to direct users to the closest web tier. It has been noted that Australian users receive

slow response times to queries.

Which changes should be made to the database tier to improve performance?

1. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region
2. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions
3. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance
4. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2

QUESTION 50

A web application runs in public and private subnets. The application architecture consists of a web tier and database tier running on Amazon EC2 instances. Both tiers run in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

1. Create new public and private subnets in the same AZ for high availability
2. Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs
3. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)
4. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ
5. Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment

QUESTION 51

An application running on an Amazon ECS container instance using the EC2 launch type needs permissions to write data to Amazon DynamoDB.

How can you assign these permissions only to the specific ECS task that is running the application?

1. Create an IAM policy with permissions to DynamoDB and attach it to the container instance
2. Create an IAM policy with permissions to DynamoDB and assign it to a task using the *taskRoleArn* parameter
3. Use a security group to allow outbound connections to DynamoDB and assign it to the container instance
4. Modify the *AmazonECSTaskExecutionRolePolicy* policy to add permissions for DynamoDB

QUESTION 52

An organization has a large amount of data on Windows (SMB) file shares in their on-premises data center. The organization would like to move data into Amazon S3. They would like to automate the migration of data over their AWS Direct Connect link.

Which AWS service can assist them?

1. AWS Database Migration Service (DMS)
2. AWS CloudFormation
3. AWS Snowball
4. AWS DataSync

QUESTION 53

The database tier of a web application is running on a Windows server on-premises. The database is a Microsoft SQL Server database. The application owner would like to migrate the database to an Amazon RDS instance.

How can the migration be executed with minimal administrative effort and downtime?

1. Use the AWS Server Migration Service (SMS) to migrate the server to Amazon EC2. Use AWS Database Migration Service (DMS) to migrate the database to RDS
2. Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS
3. Use AWS DataSync to migrate the data from the database to Amazon S3. Use AWS Database Migration Service (DMS) to migrate the database to RDS
4. Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS. Use the Schema Conversion Tool (SCT) to enable conversion from Microsoft SQL Server to Amazon RDS

QUESTION 54

A new application will run across multiple Amazon ECS tasks. Front-end application logic will process data and then pass that data to a back-end ECS task to perform further processing and write the data to a datastore. The Architect would like to reduce interdependencies so failures do not impact other components.

Which solution should the Architect use?

1. Create an Amazon Kinesis Firehose delivery stream and configure the front-end to add data to the stream and the back-end to read data from the stream
2. Create an Amazon Kinesis Firehose delivery stream that delivers data to an Amazon S3 bucket, configure the front-end to write data to the stream and the back-end to read data from Amazon S3
3. Create an Amazon SQS queue that pushes messages to the back-end. Configure the front-end to add messages to the queue
4. Create an Amazon SQS queue and configure the front-end to add messages to the queue and the back-end to poll the queue for messages

QUESTION 55

Amazon EC2 instances in a development environment run between 9am and 5pm Monday-Friday. Production instances run 24/7. Which pricing models should be used to optimize cost and ensure capacity is available? (Select TWO.)

1. Use Spot instances for the development environment
2. Use Reserved instances for the development environment
3. On-demand capacity reservations for the development environment
4. Use Reserved instances for the production environment
5. Use On-Demand instances for the production environment

QUESTION 56

An application running on Amazon EC2 needs to asynchronously invoke an AWS Lambda function to perform data processing. The services should be decoupled.

Which service can be used to decouple the compute services?

1. AWS Config
2. Amazon SNS
3. Amazon MQ
4. AWS Step Functions

QUESTION 57

A company wishes to restrict access to their Amazon DynamoDB table to specific, private source IP addresses from their VPC. What should be done to secure access to the table?

1. Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)
2. Create a gateway VPC endpoint and add an entry to the route table
3. Create the Amazon DynamoDB table in the VPC
4. Create an AWS VPN connection to the Amazon DynamoDB endpoint

QUESTION 58

An AWS Organization has an OU with multiple member accounts in it. The company needs to restrict the ability to launch only specific Amazon EC2 instance types. How can this policy be applied across the accounts with the least effort?

1. Create an SCP with an allow rule that allows launching the specific instance types
2. Create an SCP with a deny rule that denies all but the specific instance types
3. Create an IAM policy to deny launching all but the specific instance types
4. Use AWS Resource Access Manager to control which launch types can be used

QUESTION 59

An Amazon RDS Read Replica is being deployed in a separate region. The master database is not encrypted but all data in the

new region must be encrypted. How can this be achieved?

1. Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica
2. Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot
3. Enabled encryption on the master DB instance, then create an encrypted cross-region Read Replica
4. Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica

QUESTION 60

A legacy tightly-coupled High Performance Computing (HPC) application will be migrated to AWS. Which network adapter type should be used?

1. Elastic Network Interface (ENI)
2. Elastic Network Adapter (ENA)
3. Elastic Fabric Adapter (EFA)
4. Elastic IP Address

QUESTION 61

A new application is to be published in multiple regions around the world. The Architect needs to ensure only 2 IP addresses need to be whitelisted. The solution should intelligently route traffic for lowest latency and provide fast regional failover.

How can this be achieved?

1. Launch EC2 instances into multiple regions behind an NLB with a static IP address
2. Launch EC2 instances into multiple regions behind an ALB and use a Route 53 failover routing policy
3. Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator
4. Launch EC2 instances into multiple regions behind an ALB and use Amazon CloudFront with a pair of static IP addresses

QUESTION 62

A manufacturing company captures data from machines running at customer sites. Currently, thousands of machines send data every 5 minutes, and this is expected to grow to hundreds of thousands of machines in the near future. The data is logged with the intent to be analyzed in the future as needed.

What is the SIMPLEST method to store this streaming data at scale?

1. Create an Amazon EC2 instance farm behind an ELB to store the data in Amazon EBS Cold HDD volumes
2. Create an Amazon SQS queue, and have the machines write to the queue
3. Create an Amazon Kinesis Firehose delivery stream to store the data in Amazon S3
4. Create an Auto Scaling Group of Amazon EC2 instances behind ELBs to write data into Amazon RDS

QUESTION 63

A recent security audit uncovered some poor deployment and configuration practices within your VPC. You need to ensure that applications are deployed in secure configurations.

How can this be achieved in the most operationally efficient manner?

1. Remove the ability for staff to deploy applications
2. Use CloudFormation with securely configured templates
3. Manually check all application configurations before deployment
4. Use AWS Inspector to apply secure configurations

QUESTION 64

An e-commerce application is hosted in AWS. The last time a new product was launched, the application experienced a performance issue due to an enormous spike in traffic. Management decided that capacity must be doubled this week after the product is launched.

What is the MOST efficient way for management to ensure that capacity requirements are met?

1. Add a Step Scaling policy

2. Add a Simple Scaling policy
3. Add a Scheduled Scaling action
4. Add Amazon EC2 Spot instances

QUESTION 65

Your company shares some HR videos stored in an Amazon S3 bucket via CloudFront. You need to restrict access to the private content so users coming from specific IP addresses can access the videos and ensure direct access via the Amazon S3 bucket is not possible.

How can this be achieved?

1. Configure CloudFront to require users to access the files using signed cookies, create an origin access identity (OAI) and instruct users to login with the OAI
2. Configure CloudFront to require users to access the files using a signed URL, create an origin access identity (OAI) and restrict access to the files in the Amazon S3 bucket to the OAI
3. Configure CloudFront to require users to access the files using signed cookies, and move the files to an encrypted EBS volume
4. Configure CloudFront to require users to access the files using a signed URL, and configure the S3 bucket as a website endpoint

SET 1: PRACTICE QUESTIONS AND ANSWERS

QUESTION 1

A company has two accounts for perform testing and each account has a single VPC: VPC-TEST1 and VPC-TEST2. The operations team require a method of securely copying files between Amazon EC2 instances in these VPCs. The connectivity should not have any single points of failure or bandwidth constraints.

Which solution should a Solutions Architect recommend?

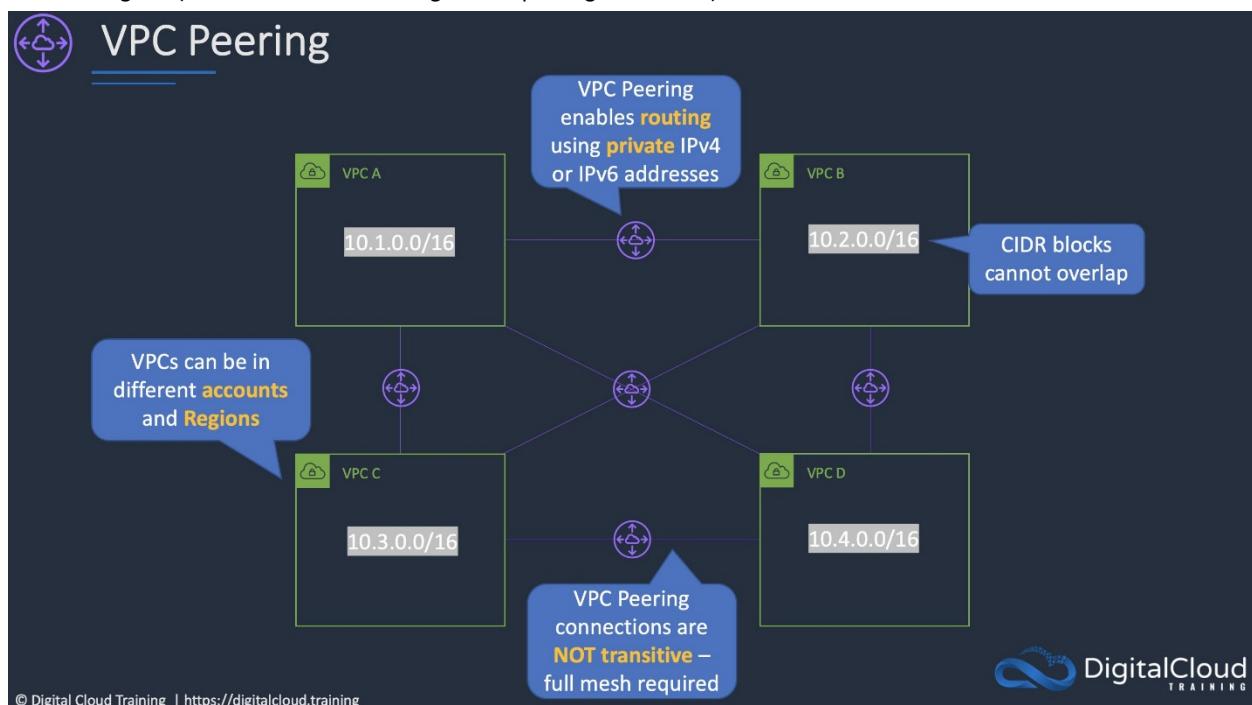
1. Create a VPC gateway endpoint for each EC2 instance and update route tables.
2. Attach a virtual private gateway to VPC-TEST1 and VPC-TEST2 and enable routing.
3. Attach a Direct Connect gateway to VPC-TEST1 and VPC-TEST2 and enable routing.
4. Create a VPC peering connection between VPC-TEST1 and VPC-TEST2.

Answer: 4

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network.

You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).



CORRECT: "Create a VPC peering connection between VPC-TEST1 and VPC-TEST2" is the correct answer.

INCORRECT: "Create a VPC gateway endpoint for each EC2 instance and update route tables" is incorrect. You cannot create VPC gateway endpoints for Amazon EC2 instances. These are used with DynamoDB and S3 only.

INCORRECT: "Attach a virtual private gateway to VPC-TEST1 and VPC-TEST2 and enable routing" is incorrect. You cannot create an AWS Managed VPN connection between two VPCs.

INCORRECT: "Attach a Direct Connect gateway to VPC-TEST1 and VPC-TEST2 and enable routing" is incorrect. Direct Connect gateway is used to connect a Direct Connect connection to multiple VPCs, it is not useful in this scenario as there is no Direct Connect connection.

References:

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 2

A Solutions Architect has deployed an application on several Amazon EC2 instances across three private subnets. The application must be made accessible to internet-based clients with the least amount of administrative effort.

How can the Solutions Architect make the application available on the internet?

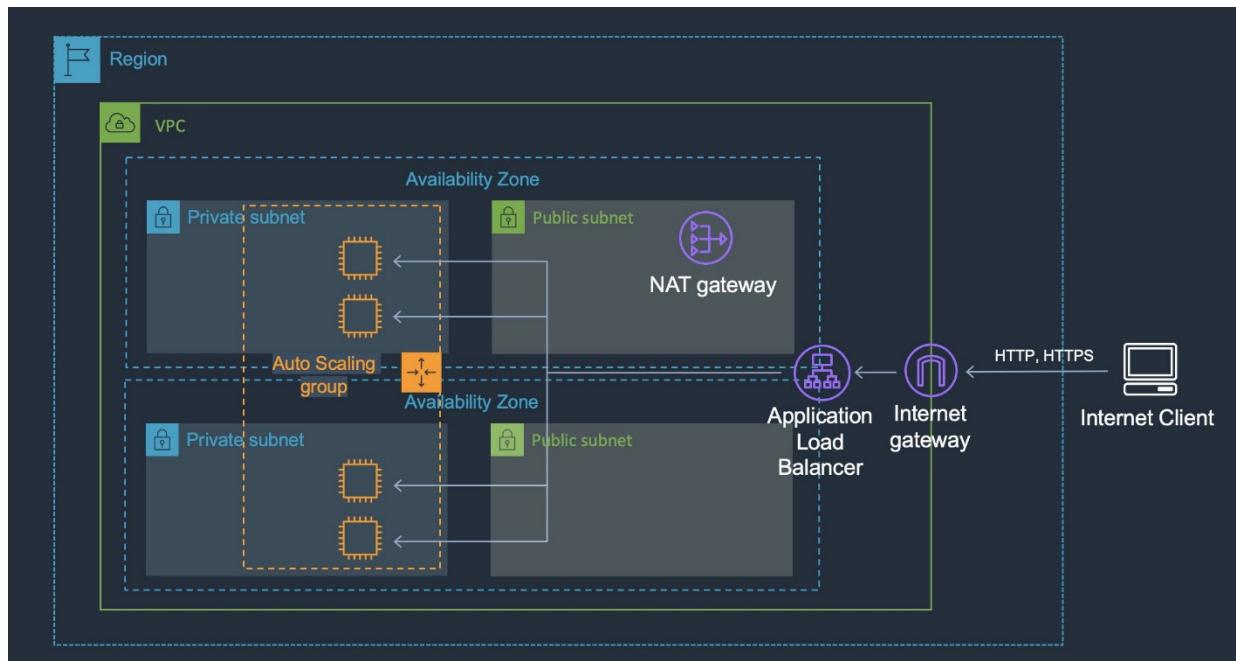
1. Create an Amazon Machine Image (AMI) of the instances in the private subnet and launch new instances from the AMI in public subnets. Create an Application Load Balancer and add the public instances to the ALB.
2. Create an Application Load Balancer and associate three public subnets from the same Availability Zones as the private instances. Add the private instances to the ALB.
3. Create an Application Load Balancer and associate three private subnets from the same Availability Zones as the private instances. Add the private instances to the ALB.
4. Create a NAT gateway in a public subnet. Add a route to the NAT gateway to the route tables of the three private subnets.

Answer: 2

Explanation:

To make the application instances accessible on the internet the Solutions Architect needs to place them behind an internet-facing Elastic Load Balancer. The way you add instances in private subnets to a public facing ELB is to add public subnets in the same AZs as the private subnets to the ELB. You can then add the instances and to the ELB and they will become targets for load balancing.

An example of this architecture is shown below:



CORRECT: "Create an Application Load Balancer and associate three public subnets from the same Availability Zones as the private instances. Add the private instances to the ALB" is the correct answer.

INCORRECT: "Create an Application Load Balancer and associate three private subnets from the same Availability Zones as the private instances. Add the private instances to the ALB" is incorrect. Public subnets in the same AZs as the private subnets must

be added to make this configuration work.

INCORRECT: "Create an Amazon Machine Image (AMI) of the instances in the private subnet and launch new instances from the AMI in public subnets. Create an Application Load Balancer and add the public instances to the ALB" is incorrect. There is no need to use an AMI to create new instances in a public subnet. You can add instances in private subnets to a public-facing ELB.

INCORRECT: "Create a NAT gateway in a public subnet. Add a route to the NAT gateway to the route tables of the three private subnets" is incorrect. A NAT gateway is used for outbound traffic not inbound traffic and cannot make the application available to internet-based clients.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 3

A video production company is planning to move some of its workloads to the AWS Cloud. The company will require around 5 TB of storage for video processing with the maximum possible I/O performance. They also require over 400 TB of extremely durable storage for storing video files and 800 TB of storage for long-term archival.

Which combinations of services should a Solutions Architect use to meet these requirements?

1. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage.
2. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage.
3. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage.
4. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage.

Answer: 1

Explanation:

The best I/O performance can be achieved by using instance store volumes for the video processing. This is safe to use for use cases where the data can be recreated from the source files so this is a good use case.

For storing data durably Amazon S3 is a good fit as it provides 99.999999999% of durability. For archival the video files can then be moved to Amazon S3 Glacier which is a low cost storage option that is ideal for long-term archival.

CORRECT: "Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage" is the correct answer.

INCORRECT: "Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage" is incorrect. EBS is not going to provide as much I/O performance as an instance store volume so is not the best choice for this use case.

INCORRECT: "Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage" is incorrect. EFS does not provide as much durability as Amazon S3 and will not be as cost-effective.

INCORRECT: "Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage" is incorrect. EBS and EFS are not the best choices here as described above.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

<https://aws.amazon.com/s3/storage-classes/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 4

A company provides a REST-based interface to an application that allows a partner company to send data in near-real time. The

application then processes the data that is received and stores it for later analysis. The application runs on Amazon EC2 instances.

The partner company has received many 503 Service Unavailable Errors when sending data to the application and the compute capacity reaches its limits and is unable to process requests when spikes in data volume occur.

Which design should a Solutions Architect implement to improve scalability?

1. Use Amazon API Gateway in front of the existing application. Create a usage plan with a quota limit for the partner company.
2. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
3. Use Amazon SQS to ingest the data. Configure the EC2 instances to process messages from the SQS queue.
4. Use Amazon SNS to ingest the data and trigger AWS Lambda functions to process the data in near-real time.

Answer: 2

Explanation:

Amazon Kinesis enables you to ingest, buffer, and process streaming data in real-time. Kinesis can handle any amount of streaming data and process data from hundreds of thousands of sources with very low latencies. This is an ideal solution for data ingestion.

To ensure the compute layer can scale to process increasing workloads, the EC2 instances should be replaced by AWS Lambda functions. Lambda can scale seamlessly by running multiple executions in parallel.

CORRECT: "Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions" is the correct answer.

INCORRECT: "Use Amazon API Gateway in front of the existing application. Create a usage plan with a quota limit for the partner company" is incorrect. A usage plan will limit the amount of data that is received and cause more errors to be received by the partner company.

INCORRECT: "Use Amazon SQS to ingest the data. Configure the EC2 instances to process messages from the SQS queue" is incorrect. Amazon Kinesis Data Streams should be used for near-real time or real-time use cases instead of Amazon SQS.

INCORRECT: "Use Amazon SNS to ingest the data and trigger AWS Lambda functions to process the data in near-real time" is incorrect. SNS is not a near-real time solution for data ingestion. SNS is used for sending notifications.

References:

<https://aws.amazon.com/kinesis/>

<https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>

QUESTION 5

A persistent database must be migrated from an on-premises server to an Amazon EC2 instances. The database requires 64,000 IOPS and, if possible, should be stored on a single Amazon EBS volume.

Which solution should a Solutions Architect recommend?

1. Use an instance from the I3 I/O optimized family and leverage instance store storage to achieve the IOPS requirement.
2. Create an Amazon EC2 instance with four Amazon EBS General Purpose SSD (gp2) volumes attached. Max out the IOPS on each volume and use a RAID 0 stripe set.
3. Create a Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (iO1) volume attached. Provision 64,000 IOPS for the volume.
4. Create an Amazon EC2 instance with two Amazon EBS Provisioned IOPS SSD (iO1) volumes attached. Provision 32,000 IOPS per volume and create a logical volume using the OS that aggregates the capacity.

Answer: 3

Explanation:

Amazon EC2 Nitro-based systems are not required for this solution but do offer advantages in performance that will help to

maximize the usage of the EBS volume. For the data storage volume an io1 volume can support up to 64,000 IOPS so a single volume with sufficient capacity (50 IOPS per GiB) can be deliver the requirements.

The current list of EBS volume types is in the table below:

	General Purpose SSD		Provisioned IOPS SSD		
Volume type	gp3	gp2	io2 Block Express ‡	io2	io1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	<ul style="list-style-type: none"> Low-latency interactive apps Development and test environments 		<p>Workloads that require:</p> <ul style="list-style-type: none"> Sub-millisecond latency Sustained IOPS performance More than 64,000 IOPS or 1,000 MiB/s of throughput 		
Volume size	1 GiB - 16 TiB		4 GiB - 64 TiB	4 GiB - 16 TiB	
Max IOPS per volume (16 KiB I/O)	16,000		256,000	64,000 †	
Max throughput per volume	1,000 MiB/s	250 MiB/s *	4,000 MiB/s	1,000 MiB/s †	
Amazon EBS Multi-attach	Not supported		Supported		
Boot volume	Supported				

CORRECT: "Create a Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Provision 64,000 IOPS for the volume" is the correct answer.

INCORRECT: "Use an instance from the I3 I/O optimized family and leverage instance store storage to achieve the IOPS requirement" is incorrect.

INCORRECT: "Create an Amazon EC2 instance with four Amazon EBS General Purpose SSD (gp2) volumes attached. Max out the IOPS on each volume and use a RAID 0 stripe set" is incorrect. This is not a good use case for gp2 volumes. It is much better to use io1 which also meets the requirement of having a single volume with 64,000 IOPS.

INCORRECT: "Create an Amazon EC2 instance with two Amazon EBS Provisioned IOPS SSD (io1) volumes attached. Provision 32,000 IOPS per volume and create a logical volume using the OS that aggregates the capacity" is incorrect. There is no need to create two volumes and aggregate capacity through the OS, the Solutions Architect can simply create a single volume with 64,000 IOPS.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 6

A company uses an Amazon RDS MySQL database instance to store customer order data. The security team have requested that SSL/TLS encryption in transit must be used for encrypting connections to the database from application servers. The data in the database is currently encrypted at rest using an AWS KMS key.

How can a Solutions Architect enable encryption in transit?

1. Enable encryption in transit using the RDS Management console and obtain a key using AWS KMS.
2. Add a self-signed certificate to the RDS DB instance. Use the certificates in all connections to the RDS DB instance.
3. Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption in transit enabled.
4. Download the AWS-provided root certificates. Use the certificates when connecting to the RDS DB instance.

Answer: 4

Explanation:

Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

You can download a root certificate from AWS that works for all Regions or you can download Region-specific intermediate certificates.

CORRECT: "Download the AWS-provided root certificates. Use the certificates when connecting to the RDS DB instance" is the correct answer.

INCORRECT: "Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption in transit enabled" is incorrect. There is no need to do this as a certificate is created when the DB instances is launched.

INCORRECT: "Enable encryption in transit using the RDS Management console and obtain a key using AWS KMS" is incorrect. You cannot enable/disable encryption in transit using the RDS management console or use a KMS key.

INCORRECT: "Add a self-signed certificate to the RDS DB instance. Use the certificates in all connections to the RDS DB instance" is incorrect. You cannot use self-signed certificates with RDS.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 7

An eCommerce company runs an application on Amazon EC2 instances in public and private subnets. The web application runs in a public subnet and the database runs in a private subnet. Both the public and private subnets are in a single Availability Zone.

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

1. Create new public and private subnets in the same AZ but in a different Amazon VPC.
2. Create an EC2 Auto Scaling group in the public subnet and use an Application Load Balancer.
3. Create an EC2 Auto Scaling group and Application Load Balancer that spans across multiple AZs.
4. Create new public and private subnets in a different AZ. Create a database using Amazon EC2 in one AZ.
5. Create new public and private subnets in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment.

Answer: 3, 5

Explanation:

High availability can be achieved by using multiple Availability Zones within the same VPC. An EC2 Auto Scaling group can then be used to launch web application instances in multiple public subnets across multiple AZs and an ALB can be used to distribute incoming load.

The database solution can be made highly available by migrating from EC2 to Amazon RDS and using a Multi-AZ deployment model. This will provide the ability to failover to another AZ in the event of a failure of the primary database or the AZ in which it runs.

CORRECT: "Create an EC2 Auto Scaling group and Application Load Balancer that spans across multiple AZs" is a correct answer.

CORRECT: "Create new public and private subnets in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment" is also a correct answer.

INCORRECT: "Create new public and private subnets in the same AZ but in a different Amazon VPC" is incorrect. You cannot use multiple VPCs for this solution as it would be difficult to manage and direct traffic (you can't load balance across VPCs).

INCORRECT: "Create an EC2 Auto Scaling group in the public subnet and use an Application Load Balancer" is incorrect. This does not achieve HA as you need multiple public subnets across multiple AZs.

INCORRECT: "Create new public and private subnets in a different AZ. Create a database using Amazon EC2 in one AZ" is incorrect. The database solution is not HA in this answer option.

References:

<https://aws.amazon.com/ec2/autoscaling/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 8

A company runs an application on six web application servers in an Amazon EC2 Auto Scaling group in a single Availability Zone. The application is fronted by an Application Load Balancer (ALB). A Solutions Architect needs to modify the infrastructure to be highly available without making any modifications to the application.

Which architecture should the Solutions Architect choose to enable high availability?

1. Create an Amazon CloudFront distribution with a custom origin across multiple Regions.
2. Modify the Auto Scaling group to use two instances across each of three Availability Zones.
3. Create a launch template that can be used to quickly create more instances in another Region.
4. Create an Auto Scaling group to launch three instances across each of two Regions.

Answer: 2

Explanation:

The only thing that needs to be changed in this scenario to enable HA is to split the instances across multiple Availability Zones. The architecture already uses Auto Scaling and Elastic Load Balancing so there is plenty of resilience to failure. Once the instances are running across multiple AZs there will be AZ-level fault tolerance as well.

CORRECT: "Modify the Auto Scaling group to use two instances across each of three Availability Zones" is the correct answer.

INCORRECT: "Create an Amazon CloudFront distribution with a custom origin across multiple Regions" is incorrect. CloudFront is not used to create HA for your application, it is used to accelerate access to media content.

INCORRECT: "Create a launch template that can be used to quickly create more instances in another Region" is incorrect. Multi-AZ should be enabled rather than multi-Region.

INCORRECT: "Create an Auto Scaling group to launch three instances across each of two Regions" is incorrect. HA can be achieved within a Region by simply enabling more AZs in the ASG. An ASG cannot launch instances in multiple Regions.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 9

A web application allows users to upload photos and add graphical elements to them. The application offers two tiers of service: free and paid. Photos uploaded by paid users should be processed before those submitted using the free tier. The photos are uploaded to an Amazon S3 bucket which uses an event notification to send the job information to Amazon SQS.

How should a Solutions Architect configure the Amazon SQS deployment to meet these requirements?

1. Use one SQS standard queue. Use batching for the paid photos and short polling for the free photos.
2. Use a separate SQS FIFO queue for each tier. Set the free queue to use short polling and the paid queue to use long polling.
3. Use a separate SQS Standard queue for each tier. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.
4. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.

Answer: 3

Explanation:

AWS recommend using separate queues when you need to provide prioritization of work. The logic can then be implemented at the application layer to prioritize the queue for the paid photos over the queue for the free photos.

CORRECT: "Use a separate SQS Standard queue for each tier. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue" is the correct answer.

INCORRECT: "Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first" is incorrect. FIFO queues preserve the order of messages but they do not prioritize messages within the queue. The orders would need to be placed into the queue in a priority order and there's no way of doing this as the messages are sent automatically through event notifications as they are received by Amazon S3.

INCORRECT: "Use one SQS standard queue. Use batching for the paid photos and short polling for the free photos" is incorrect. Batching adds efficiency but it has nothing to do with ordering or priority.

INCORRECT: "Use a separate SQS FIFO queue for each tier. Set the free queue to use short polling and the paid queue to use long polling" is incorrect. Short polling and long polling are used to control the amount of time the consumer process waits before closing the API call and trying again. Polling should be configured for efficiency of API calls and processing of messages but does not help with message prioritization.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-how-it-works.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 10

A company has deployed a new website on Amazon EC2 instances behind an Application Load Balancer (ALB). Amazon Route 53 is used for the DNS service. The company has asked a Solutions Architect to create a backup website with support contact details that users will be directed to automatically if the primary website is down.

How should the Solutions Architect deploy this solution cost-effectively?

1. Configure a static website using Amazon S3 and create a Route 53 weighted routing policy.
2. Deploy the backup website on EC2 and ALB in another Region and use Route 53 health checks for failover routing.
3. Create the backup website on EC2 and ALB in another Region and create an AWS Global Accelerator endpoint.
4. Configure a static website using Amazon S3 and create a Route 53 failover routing policy.

Answer: 4

Explanation:

The most cost-effective solution is to create a static website using an Amazon S3 bucket and then use a failover routing policy in Amazon Route 53. With a failover routing policy users will be directed to the main website as long as it is responding to health checks successfully.

If the main website fails to respond to health checks (it's down), Route 53 will begin to direct users to the backup website running on the Amazon S3 bucket. It's important to set the TTL on the Route 53 records appropriately to ensure that users resolve the failover address within a short time.

CORRECT: "Configure a static website using Amazon S3 and create a Route 53 failover routing policy" is the correct answer.

INCORRECT: "Configure a static website using Amazon S3 and create a Route 53 weighted routing policy" is incorrect. Weighted routing is used when you want to send a percentage of traffic between multiple endpoints. In this case all traffic should go to the primary until it fails, then all should go to the backup.

INCORRECT: "Deploy the backup website on EC2 and ALB in another Region and use Route 53 health checks for failover routing" is incorrect. This is not a cost-effective solution for the backup website. It can be implemented using Route 53 failover routing which uses health checks but would be an expensive option.

INCORRECT: "Create the backup website on EC2 and ALB in another Region and create an AWS Global Accelerator endpoint" is incorrect. Global Accelerator is used for performance as it directs traffic to the nearest healthy endpoint. It is not useful for failover in this scenario and is also a very expensive solution.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon->

QUESTION 11

A company requires that all AWS IAM user accounts have specific complexity requirements and minimum password length.

How should a Solutions Architect accomplish this?

1. Set a password policy for each IAM user in the AWS account.
2. Set a password policy for the entire AWS account.
3. Create an IAM policy that enforces the requirements and apply it to all users.
4. Use an AWS Config rule to enforce the requirements when creating user accounts.

Answer: 2

Explanation:

The easiest way to enforce this requirement is to update the password policy that applies to the entire AWS account. When you create or change a password policy, most of the password policy settings are enforced the next time your users change their passwords. However, some of the settings are enforced immediately such as the password expiration period.

CORRECT: "Set a password policy for the entire AWS account" is the correct answer.

INCORRECT: "Set a password policy for each IAM user in the AWS account" is incorrect. There's no need to set an individual password policy for each user, it will be easier to set the policy for everyone.

INCORRECT: "Create an IAM policy that enforces the requirements and apply it to all users" is incorrect. As there is no specific targeting required it is easier to update the account password policy.

INCORRECT: "Use an AWS Config rule to enforce the requirements when creating user accounts" is incorrect. You cannot use AWS Config to enforce the password requirements at the time of creating a user account.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 12

A company runs a dynamic website that is hosted on an on-premises server in the United States. The company is expanding to Europe and is investigating how they can optimize the performance of the website for European users. The website's backed must remain in the United States. The company requires a solution that can be implemented within a few days.

What should a Solutions Architect recommend?

1. Use Amazon CloudFront with Lambda@Edge to direct traffic to an on-premises origin.
2. Launch an Amazon EC2 instance in an AWS Region in the United States and migrate the website to it.
3. Migrate the website to Amazon S3. Use cross-Region replication between Regions and a latency-based Route 53 policy.
4. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

Answer: 4

Explanation:

A custom origin can point to an on-premises server and CloudFront is able to cache content for dynamic websites. CloudFront can provide performance optimizations for custom origins even if they are running on on-premises servers. These include persistent TCP connections to the origin, SSL enhancements such as Session tickets and OCSP stapling.

Additionally, connections are routed from the nearest Edge Location to the user across the AWS global network. If the on-premises server is connected via a Direct Connect (DX) link this can further improve performance.

CORRECT: "Use Amazon CloudFront with a custom origin pointing to the on-premises servers" is the correct answer.

INCORRECT: "Use Amazon CloudFront with Lambda@Edge to direct traffic to an on-premises origin" is incorrect. Lambda@Edge is not used to direct traffic to on-premises origins.

INCORRECT: "Launch an Amazon EC2 instance in an AWS Region in the United States and migrate the website to it" is incorrect.

This would not necessarily improve performance for European users.

INCORRECT: "Migrate the website to Amazon S3. Use cross-Region replication between Regions and a latency-based Route 53 policy" is incorrect. You cannot host dynamic websites on Amazon S3 (static only).

References:

<https://aws.amazon.com/cloudfront/dynamic-content/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 13

A company runs an application in an on-premises data center that collects environmental data from production machinery. The data consists of JSON files stored on network attached storage (NAS) and around 5 TB of data is collected each day. The company must upload this data to Amazon S3 where it can be processed by an analytics application. The data must be transferred securely.

Which solution offers the MOST reliable and time-efficient data transfer?

1. AWS Database Migration Service over the Internet.
2. Amazon S3 Transfer Acceleration over the Internet.
3. AWS DataSync over AWS Direct Connect.
4. Multiple AWS Snowcone devices.

Answer: 3

Explanation:

The most reliable and time-efficient solution that keeps the data secure is to use AWS DataSync and synchronize the data from the NAS device directly to Amazon S3. This should take place over an AWS Direct Connect connection to ensure reliability, speed, and security.

AWS DataSync can copy data between Network File System (NFS) shares, Server Message Block (SMB) shares, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Elastic File System (Amazon EFS) file systems, and Amazon FSx for Windows File Server file systems.

CORRECT: "AWS DataSync over AWS Direct Connect" is the correct answer.

INCORRECT: "AWS Database Migration Service over the Internet" is incorrect. DMS is for migrating databases, not files.

INCORRECT: "Amazon S3 Transfer Acceleration over the Internet" is incorrect. The Internet does not offer the reliability, speed or performance that this company requires.

INCORRECT: "Multiple AWS Snowcone devices" is incorrect. This is not a time-efficient approach as it can take time to ship these devices in both directions.

References:

<https://aws.amazon.com/datasync/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-database-migration-service/>

QUESTION 14

A company runs an application on an Amazon EC2 instance that requires 250 GB of storage space. The application is not used often and has small spikes in usage on weekday mornings and afternoons. The disk I/O can vary with peaks hitting a maximum of 3,000 IOPS. A Solutions Architect must recommend the most cost-effective storage solution that delivers the performance required.

Which configuration should the Solutions Architect recommend?

Which solution should the solutions architect recommend?

1. Amazon EBS Cold HDD (sc1)
2. Amazon EBS General Purpose SSD (gp2)

3. Amazon EBS Provisioned IOPS SSD (i01)
4. Amazon EBS Throughput Optimized HDD (st1)

Answer: 2

Explanation:

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time.

Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

In this configuration the volume will provide a baseline performance of 750 IOPS but will always be able to burst to the required 3,000 IOPS during periods of increased traffic.

CORRECT: "Amazon EBS General Purpose SSD (gp2)" is the correct answer.

INCORRECT: "Amazon EBS Provisioned IOPS SSD (i01)" is incorrect. The i01 volume type will be more expensive and is not necessary for the performance levels required.

INCORRECT: "Amazon EBS Cold HDD (sc1)" is incorrect. The sc1 volume type is not going to deliver the performance requirements as it cannot burst to 3,000 IOPS.

INCORRECT: "Amazon EBS Throughput Optimized HDD (st1)" is incorrect. The st1 volume type is not going to deliver the performance requirements as it cannot burst to 3,000 IOPS.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 15

A company offers an online product brochure that is delivered from a static website running on Amazon S3. The company's customers are mainly in the United States, Canada, and Europe. The company is looking to cost-effectively reduce the latency for users in these regions.

What is the most cost-effective solution to these requirements?

1. Create an Amazon CloudFront distribution that uses origins in U.S, Canada and Europe.
2. Create an Amazon CloudFront distribution and use Lambda@Edge to run the website's data processing closer to the users.
3. Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Europe.
4. Create an Amazon CloudFront distribution and set the price class to use all Edge Locations for best performance.

Answer: 3

Explanation:

With Amazon CloudFront you can set the price class to determine where in the world the content will be cached. One of the price classes is "U.S, Canada and Europe" and this is where the company's users are located. Choosing this price class will result in lower costs and better performance for the company's users.

CORRECT: "Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Europe." is the correct answer.

INCORRECT: "Create an Amazon CloudFront distribution and set the price class to use all Edge Locations for best performance" is incorrect. This will be more expensive as it will cache content in Edge Locations all over the world.

INCORRECT: "Create an Amazon CloudFront distribution that uses origins in U.S, Canada and Europe" is incorrect. The origin can be in one place, there's no need to add origins in different Regions. The price class should be used to limit the caching of the content to reduce cost.

INCORRECT: "Create an Amazon CloudFront distribution and use Lambda@Edge to run the website's data processing closer to the users" is incorrect. Lambda@Edge will not assist in this situation as there is no data processing required, the content from the static website must simply be cached at an edge location.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PriceClass.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 16

A developer created an application that uses Amazon EC2 and an Amazon RDS MySQL database instance. The developer stored the database user name and password in a configuration file on the root EBS volume of the EC2 application instance. A Solutions Architect has been asked to design a more secure solution.

What should the Solutions Architect do to achieve this requirement?

1. Move the configuration file to an Amazon S3 bucket. Create an IAM role with permission to the bucket and attach it to the EC2 instance.
2. Attach an additional volume to the EC2 instance with encryption enabled. Move the configuration file to the encrypted volume.
3. Install an Amazon-trusted root certificate on the application instance and use SSL/TLS encrypted connections to the database.
4. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.

Answer: 4

Explanation:

The key problem here is having plain text credentials stored in a file. Even if you encrypt the volume there is still a security risk as the credentials are loaded by the application and passed to RDS.

The best way to secure this solution is to get rid of the credentials completely by using an IAM role instead. The IAM role can be assigned permissions to the database instance and can be attached to the EC2 instance. The instance will then obtain temporary security credentials from AWS STS which is much more secure.

CORRECT: "Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance" is the correct answer.

INCORRECT: "Move the configuration file to an Amazon S3 bucket. Create an IAM role with permission to the bucket and attach it to the EC2 instance" is incorrect. This just relocates the file; the contents are still unsecured and must be loaded by the application and passed to RDS. This is an insecure process.

INCORRECT: "Attach an additional volume to the EC2 instance with encryption enabled. Move the configuration file to the encrypted volume" is incorrect. This will only encrypt the file at rest, it still must be read, and the contents passed to RDS which is insecure.

INCORRECT: "Install an Amazon-trusted root certificate on the application instance and use SSL/TLS encrypted connections to the database" is incorrect. The file is still unsecured on the EBS volume so encrypting the credentials in an encrypted channel between the EC2 instance and RDS does not solve all security issues.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 17

A financial services company has a web application with an application tier running in the U.S and Europe. The database tier consists of a MySQL database running on Amazon EC2 in us-west-1. Users are directed to the closest application tier using Route 53 latency-based routing. The users in Europe have reported poor performance when running queries.

Which changes should a Solutions Architect make to the database tier to improve performance?

1. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
2. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure the application tier in Europe to use the local reader endpoint.

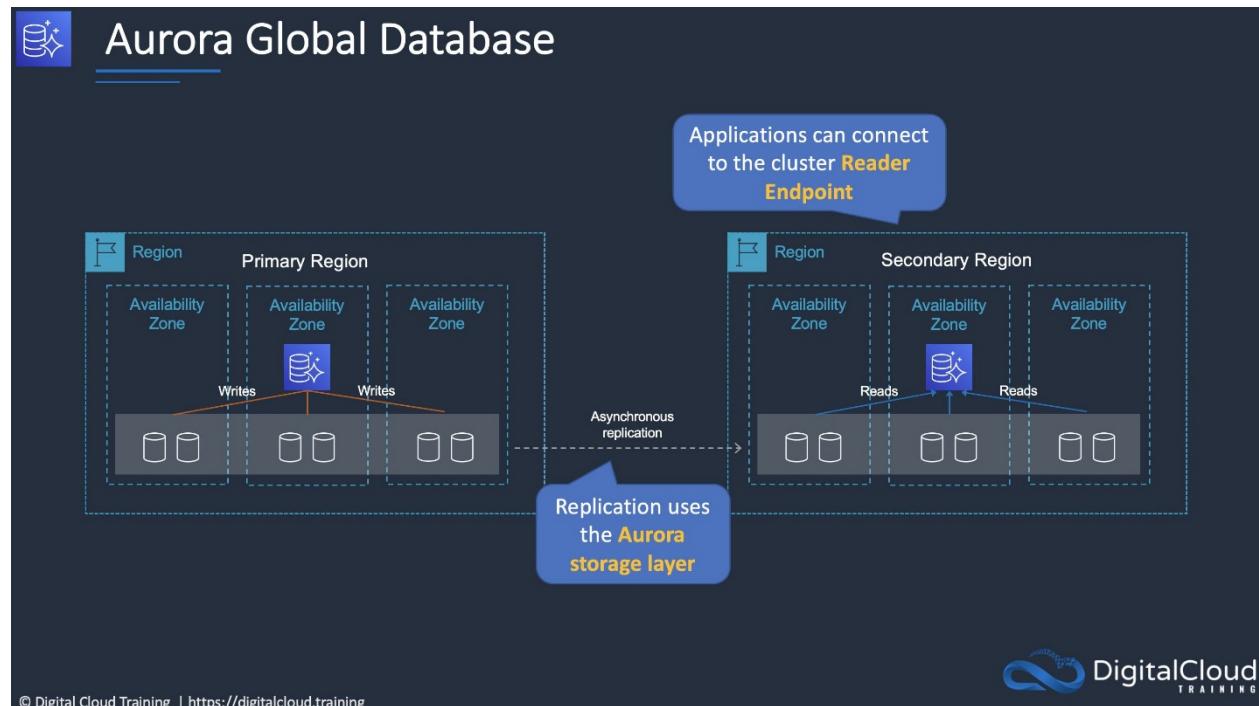
3. Migrate the database to Amazon RedShift. Use AWS DMS to synchronize data. Configure applications to use the RedShift data warehouse for queries.
4. Create an Amazon RDS Read Replica in one of the European regions. Configure the application tier in Europe to use the read replica for queries.

Answer: 2

Explanation:

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages.

A global database can be configured in the European region and then the application tier in Europe will need to be configured to use the local database for reads/queries. The diagram below depicts an Aurora Global Database deployment.



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure the application tier in Europe to use the local reader endpoint" is the correct answer.

INCORRECT: "Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions" is incorrect. You cannot configure a multi-AZ DB instance to run in another Region, it must be in the same Region but in a different Availability Zone.

INCORRECT: "Migrate the database to Amazon RedShift. Use AWS DMS to synchronize data. Configure applications to use the RedShift data warehouse for queries" is incorrect. RedShift is a data warehouse and used for running analytics queries on data that is exported from transactional database systems. It should not be used to reduce latency for users of a database, and is not a live copy of the data.

INCORRECT: "Create an Amazon RDS Read Replica in one of the European regions. Configure the application tier in Europe to use the read replica for queries" is incorrect. You cannot create an RDS Read Replica of a database that is running on Amazon EC2. You can only create read replicas of databases running on Amazon RDS.

References:

<https://aws.amazon.com/rds/aurora/global-database/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 18

A company runs an application that uses an Amazon RDS PostgreSQL database. The database is currently not encrypted. A Solutions Architect has been instructed that due to new compliance requirements all existing and new data in the database must be encrypted. The database experiences high volumes of changes and no data can be lost.

How can the Solutions Architect enable encryption for the database without incurring any data loss?

1. Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot. Configure the application to use the new DB endpoint.
2. Create an RDS read replica and specify an encryption key. Promote the encrypted read replica to primary. Update the application to point to the new RDS DB endpoint.
3. Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs.
4. Update the RDS DB to Multi-AZ mode and enable encryption for the standby replica. Perform a failover to the standby instance and then delete the unencrypted RDS DB instance.

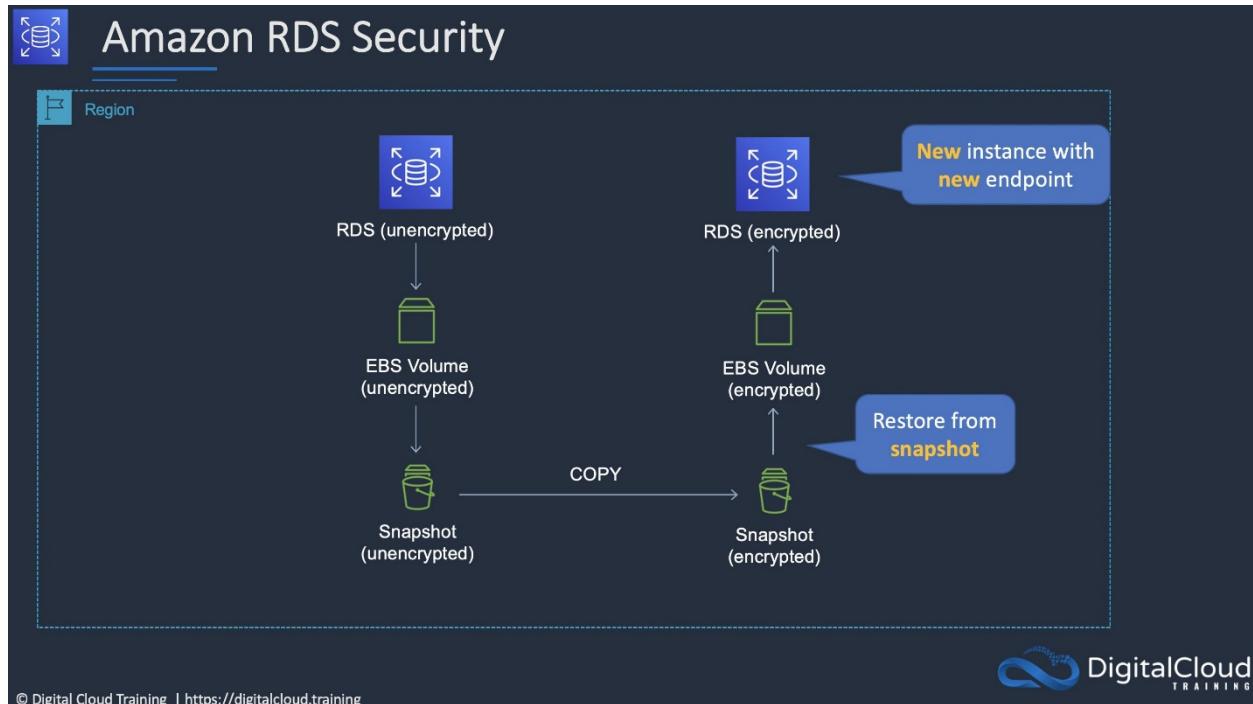
Answer: 3

Explanation:

You cannot change the encryption status of an existing RDS DB instance. Encryption must be specified when creating the RDS DB instance. The best way to encrypt an existing database is to take a snapshot, encrypt a copy of the snapshot and restore the snapshot to a new RDS DB instance. This results in an encrypted database that is a new instance. Applications must be updated to use the new RDS DB endpoint.

In this scenario as there is a high rate of change, the databases will be out of sync by the time the new copy is created and is functional. The best way to capture the changes between the source (unencrypted) and destination (encrypted) DB is to use AWS Database Migration Service (DMS) to synchronize the data.

The slide below depicts the process for encrypting an unencrypted RDS DB instance:



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs" is the correct answer.

INCORRECT: "Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot. Configure the application to use the new DB endpoint" is incorrect. This answer creates an encrypted DB instance but does not synchronize the data.

INCORRECT: "Create an RDS read replica and specify an encryption key. Promote the encrypted read replica to primary. Update the application to point to the new RDS DB endpoint" is incorrect. You cannot create an encrypted read replica of an unencrypted RDS DB. The read replica will always have the same encryption status as the RDS DB it is created from.

INCORRECT: "Update the RDS DB to Multi-AZ mode and enable encryption for the standby replica. Perform a failover to the standby instance and then delete the unencrypted RDS DB instance" is incorrect. You also cannot have an encrypted Multi-AZ standby instance of an unencrypted RDS DB.

References:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 19

A company runs an application in a factory that has a small rack of physical compute resources. The application stores data on a network attached storage (NAS) device using the NFS protocol. The company requires a daily offsite backup of the application data.

Which solution can a Solutions Architect recommend to meet this requirement?

1. Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
2. Use an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
3. Use an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.
4. Create an IPSec VPN to AWS and configure the application to mount the Amazon EFS file system. Run a copy job to backup the data to EFS.

Answer: 1

Explanation:

The AWS Storage Gateway Hardware Appliance is a physical, standalone, validated server configuration for on-premises deployments. It comes pre-loaded with Storage Gateway software, and provides all the required CPU, memory, network, and SSD cache resources for creating and configuring File Gateway, Volume Gateway, or Tape Gateway.

A file gateway is the correct type of appliance to use for this use case as it is suitable for mounting via the NFS and SMB protocols.

CORRECT: "Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3" is the correct answer.

INCORRECT: "Use an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3" is incorrect. Volume gateways are used for block-based storage and this solution requires NFS (file-based storage).

INCORRECT: "Use an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3" is incorrect. Volume gateways are used for block-based storage and this solution requires NFS (file-based storage).

INCORRECT: "Create an IPSec VPN to AWS and configure the application to mount the Amazon EFS file system. Run a copy job to backup the data to EFS" is incorrect. It would be better to use a Storage Gateway which will automatically take care of synchronizing a copy of the data to AWS.

References:

<https://aws.amazon.com/storagegateway/hardware-appliance/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

QUESTION 20

A company is deploying a fleet of Amazon EC2 instances running Linux across multiple Availability Zones within an AWS Region.

The application requires a data storage solution that can be accessed by all of the EC2 instances simultaneously. The solution must be highly scalable and easy to implement. The storage must be mounted using the NFS protocol.

Which solution meets these requirements?

1. Create an Amazon S3 bucket and create an S3 gateway endpoint to allow access to the file system using the NFS protocol.
2. Create an Amazon EFS file system with mount targets in each Availability Zone. Configure the application instances to mount the file system.
3. Create an Amazon EBS volume and use EBS Multi-Attach to mount the volume to all EC2 instances across each Availability Zone.
4. Create an Amazon RDS database and store the data in a BLOB format. Point the application instances to the RDS endpoint.

Answer: 2

Explanation:

Amazon EFS provides scalable file storage for use with Amazon EC2. You can use an EFS file system as a common data source for workloads and applications running on multiple instances. The EC2 instances can run in multiple AZs within a Region and the NFS protocol is used to mount the file system.

With EFS you can create mount targets in each AZ for lower latency. The application instances in each AZ will mount the file system using the local mount target.

CORRECT: "Create an Amazon EFS file system with mount targets in each Availability Zone. Configure the application instances to mount the file system" is the correct answer.

INCORRECT: "Create an Amazon S3 bucket and create an S3 gateway endpoint to allow access to the file system using the NFS protocol" is incorrect. You cannot use NFS with S3 or with gateway endpoints.

INCORRECT: "Create an Amazon EBS volume and use EBS Multi-Attach to mount the volume to all EC2 instances across each Availability Zone" is incorrect. You cannot use Amazon EBS Multi-Attach across multiple AZs.

INCORRECT: "Create an Amazon RDS database and store the data in a BLOB format. Point the application instances to the RDS endpoint" is incorrect. This is not a suitable storage solution for a file system that is mounted over NFS.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEFS.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 21

A company is working with a strategic partner that has an application that must be able to send messages to one of the company's Amazon SQS queues. The partner company has its own AWS account.

How can a Solutions Architect provide least privilege access to the partner?

1. Create a user account that and grant the sqs:SendMessage permission for Amazon SQS. Share the credentials with the partner company.
2. Create a cross-account role with access to all SQS queues and use the partner's AWS account in the trust document for the role.
3. Update the permission policy on the SQS queue to grant all permissions to the partner's AWS account.
4. Update the permission policy on the SQS queue to grant the sqs:SendMessage permission to the partner's AWS account.

Answer: 4

Explanation:

Amazon SQS supports resource-based policies. The best way to grant the permissions using the principle of least privilege is to use a resource-based policy attached to the SQS queue that grants the partner company's AWS account the sqs:SendMessage privilege.

The following policy is an example of how this could be configured:

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement": [
    {
      "Sid": "Queue1_SendMessage",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "111122223333"
        ]
      },
      "Action": "sns:SendMessage",
      "Resource": "arn:aws:sns:us-east-2:444455556666:queue1"
    }
  ]
}
```

CORRECT: "Update the permission policy on the SQS queue to grant the sqs:SendMessage permission to the partner's AWS account" is the correct answer.

INCORRECT: "Create a user account that and grant the sqs:SendMessage permission for Amazon SQS. Share the credentials with the partner company" is incorrect. This would provide the permissions for all SQS queues, not just the queue the partner company should be able to access.

INCORRECT: "Create a cross-account role with access to all SQS queues and use the partner's AWS account in the trust document for the role" is incorrect. This would provide access to all SQS queues and the partner company should only be able to access one SQS queue.

INCORRECT: "Update the permission policy on the SQS queue to grant all permissions to the partner's AWS account" is incorrect. This provides too many permissions; the partner company only needs to send messages to the queue.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-examples-of-sqs-policies.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 22

A company is investigating methods to reduce the expenses associated with on-premises backup infrastructure. The Solutions Architect wants to reduce costs by eliminating the use of physical backup tapes. It is a requirement that existing backup applications and workflows should continue to function.

What should the Solutions Architect recommend?

1. Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL).
2. Create an Amazon EFS file system and connect the backup applications using the NFS protocol.
3. Create an Amazon EFS file system and connect the backup applications using the iSCSI protocol.
4. Connect the backup applications to an AWS Storage Gateway using the iSCSI protocol.

Answer: 1

Explanation:

The AWS Storage Gateway Tape Gateway enables you to replace using physical tapes on premises with virtual tapes in AWS

without changing existing backup workflows. Tape Gateway emulates physical tape libraries, removes the cost and complexity of managing physical tape infrastructure, and provides more durability than physical tapes.



CORRECT: "Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL)" is the correct answer.

INCORRECT: "Create an Amazon EFS file system and connect the backup applications using the NFS protocol" is incorrect. The NFS protocol is used by AWS Storage Gateway File Gateways but these do not provide virtual tape functionality that is suitable for replacing the existing backup infrastructure.

INCORRECT: "Create an Amazon EFS file system and connect the backup applications using the iSCSI protocol" is incorrect. The NFS protocol is used by AWS Storage Gateway File Gateways but these do not provide virtual tape functionality that is suitable for replacing the existing backup infrastructure.

INCORRECT: "Connect the backup applications to an AWS Storage Gateway using the NFS protocol" is incorrect. The iSCSI protocol is used by AWS Storage Gateway Volume Gateways but these do not provide virtual tape functionality that is suitable for replacing the existing backup infrastructure.

References:

<https://aws.amazon.com/storagegateway/vtl/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

QUESTION 23

A Solutions Architect has been tasked with re-deploying an application running on AWS to enable high availability. The application processes messages that are received in an ActiveMQ queue running on a single Amazon EC2 instance. Messages are then processed by a consumer application running on Amazon EC2. After processing the messages the consumer application writes results to a MySQL database running on Amazon EC2.

Which architecture offers the highest availability and low operational complexity?

1. Deploy a second Active MQ server to another Availability Zone. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone.
2. Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone.
3. Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.
4. Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Create an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use an Amazon RDS MySQL database with Multi-AZ enabled.

Answer: 4

Explanation:

The correct answer offers the highest availability as it includes Amazon MQ active/standby brokers across two AZs, an Auto Scaling group across two AZs and a Multi-AZ Amazon RDS MySQL database deployment.

This architecture not only offers the highest availability it is also operationally simple as it maximizes the usage of managed services.

CORRECT: "Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Create an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use an Amazon RDS MySQL database with Multi-AZ enabled" is the correct answer.

INCORRECT: "Deploy a second Active MQ server to another Availability Zone. Launch an additional consumer EC2 instance in

another Availability Zone. Use MySQL database replication to another Availability Zone" is incorrect. This architecture does not offer the highest availability as it does not use Auto Scaling. It is also not the most operationally efficient architecture as it does not use AWS managed services.

INCORRECT: "Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone" is incorrect. This architecture does not use Auto Scaling for best HA or the RDS managed service.

INCORRECT: "Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled" is incorrect. This solution does not use Auto Scaling.

References:

<https://aws.amazon.com/architecture/well-architected/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-mq/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 24

Storage capacity has become an issue for a company that runs application servers on-premises. The servers are connected to a combination of block storage and NFS storage solutions. The company requires a solution that supports local caching without re-architecting its existing applications.

Which combination of changes can the company make to meet these requirements? (Select TWO.)

1. Use an AWS Storage Gateway file gateway to replace the NFS storage.
2. Use the mount command on servers to mount Amazon S3 buckets using NFS.
3. Use AWS Direct Connect and mount an Amazon FSx for Windows File Server using iSCSI.
4. Use an AWS Storage Gateway volume gateway to replace the block storage.
5. Use Amazon Elastic File System (EFS) volumes to replace the block storage.

Answer: 1, 4

Explanation:

In this scenario the company should use cloud storage to replace the existing storage solutions that are running out of capacity. The on-premises servers mount the existing storage using block protocols (iSCSI) and file protocols (NFS). As there is a requirement to avoid re-architecting existing applications these protocols must be used in the revised solution.

The AWS Storage Gateway volume gateway should be used to replace the block-based storage systems as it is mounted over iSCSI and the file gateway should be used to replace the NFS file systems as it uses NFS.

CORRECT: "Use an AWS Storage Gateway file gateway to replace the NFS storage" is a correct answer.

CORRECT: "Use an AWS Storage Gateway volume gateway to replace the block storage" is a correct answer.

INCORRECT: "Use the mount command on servers to mount Amazon S3 buckets using NFS" is incorrect. You cannot mount S3 buckets using NFS as it is an object-based storage system (not file-based) and uses an HTTP REST API.

INCORRECT: "Use AWS Direct Connect and mount an Amazon FSx for Windows File Server using iSCSI" is incorrect. You cannot mount FSx for Windows File Server file systems using iSCSI, you must use SMB.

INCORRECT: "Use Amazon Elastic File System (EFS) volumes to replace the block storage" is incorrect. You cannot use EFS to replace block storage as it uses NFS rather than iSCSI.

References:

<https://docs.aws.amazon.com/storagegateway/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

QUESTION 25

A company hosts an application on Amazon EC2 instances behind Application Load Balancers in several AWS Regions. Distribution rights for the content require that users in different geographies must be served content from specific regions.

Which configuration meets these requirements?

1. Create Amazon Route 53 records with a geolocation routing policy.
2. Create Amazon Route 53 records with a geoproximity routing policy.
3. Configure Amazon CloudFront with multiple origins and AWS WAF.
4. Configure Application Load Balancers with multi-Region routing.

Answer: 1

Explanation:

To protect the distribution rights of the content and ensure that users are directed to the appropriate AWS Region based on the location of the user, the geolocation routing policy can be used with Amazon Route 53.

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from.

When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights.

CORRECT: "Create Amazon Route 53 records with a geolocation routing policy" is the correct answer.

INCORRECT: "Create Amazon Route 53 records with a geoproximity routing policy" is incorrect. Use this routing policy 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.

INCORRECT: "Configure Amazon CloudFront with multiple origins and AWS WAF" is incorrect. AWS WAF protects against web exploits but will not assist with directing users to different content (from different origins).

INCORRECT: "Configure Application Load Balancers with multi-Region routing" is incorrect. There is no such thing as multi-Region routing for ALBs.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

QUESTION 26

A company plans to make an Amazon EC2 Linux instance unavailable outside of business hours to save costs. The instance is backed by an Amazon EBS volume. There is a requirement that the contents of the instance's memory must be preserved when it is made unavailable.

How can a solutions architect meet these requirements?

1. Stop the instance outside business hours. Start the instance again when required.
2. Hibernate the instance outside business hours. Start the instance again when required.
3. Use Auto Scaling to scale down the instance outside of business hours. Scale up the instance when required.
4. Terminate the instance outside business hours. Recover the instance again when required.

Answer: 2

Explanation:

When you hibernate an instance, Amazon EC2 signals the operating system to perform hibernation (suspend-to-disk). Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. Amazon EC2 persists the instance's EBS root volume and any attached EBS data volumes. When you start your instance:

- The EBS root volume is restored to its previous state

- The RAM contents are reloaded
- The processes that were previously running on the instance are resumed
- Previously attached data volumes are reattached and the instance retains its instance ID

CORRECT: "Hibernate the instance outside business hours. Start the instance again when required" is the correct answer.

INCORRECT: "Stop the instance outside business hours. Start the instance again when required" is incorrect. When an instance is stopped the operating system is shut down and the contents of memory will be lost.

INCORRECT: "Use Auto Scaling to scale down the instance outside of business hours. Scale out the instance when required" is incorrect. Auto Scaling scales does not scale up and down, it scales in by terminating instances and out by launching instances. When scaling out new instances are launched and no state will be available from terminated instances.

INCORRECT: "Terminate the instance outside business hours. Recover the instance again when required" is incorrect. You cannot recover terminated instances, you can recover instances that have become impaired in some circumstances.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 27

A Microsoft Windows file server farm uses Distributed File System Replication (DFSR) to synchronize data in an on-premises environment. The infrastructure is being migrated to the AWS Cloud.

Which service should the solutions architect use to replace the file server farm?

1. Amazon EFS
2. Amazon EBS
3. AWS Storage Gateway
4. Amazon FSx

Answer: 4

Explanation:

Amazon FSx for Windows file server supports DFS namespaces and DFS replication. This is the best solution for replacing the on-premises infrastructure. Note the limitations for deployment:

Deployment type	SSD storage	HDD storage	DFS namespaces	DFS replication	Custom DNS names	CA shares
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect. You cannot replace a Windows file server farm with EFS as it uses a completely different protocol.

INCORRECT: "Amazon EBS" is incorrect. Amazon EBS provides block-based volumes that are attached to EC2 instances. It cannot be used for replacing a shared Windows file server farm using DFSR.

INCORRECT: "AWS Storage Gateway" is incorrect. This service is used for providing cloud storage solutions for on-premises servers. In this case the infrastructure is being migrated into the AWS Cloud.

References:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 28

An eCommerce application consists of three tiers. The web tier includes EC2 instances behind an Application Load balancer, the middle tier uses EC2 instances and an Amazon SQS queue to process orders, and the database tier consists of an Auto Scaling DynamoDB table. During busy periods customers have complained about delays in the processing of orders. A Solutions Architect has been tasked with reducing processing times.

Which action will be MOST effective in accomplishing this requirement?

1. Replace the Amazon SQS queue with Amazon Kinesis Data Firehose.
2. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.
3. Use Amazon DynamoDB Accelerator (DAX) in front of the DynamoDB backend tier.
4. Add an Amazon CloudFront distribution with a custom origin to cache the responses for the web tier.

Answer: 2

Explanation:

The most likely cause of the processing delays is insufficient instances in the middle tier where the order processing takes place. The most effective solution to reduce processing times in this case is to scale based on the backlog per instance (number of messages in the SQS queue) as this reflects the amount of work that needs to be done.

CORRECT: "Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth" is the correct answer.

INCORRECT: "Replace the Amazon SQS queue with Amazon Kinesis Data Firehose" is incorrect. The issue is not the efficiency of queuing messages but the processing of the messages. In this case scaling the EC2 instances to reflect the workload is a better solution.

INCORRECT: "Use Amazon DynamoDB Accelerator (DAX) in front of the DynamoDB backend tier" is incorrect. The DynamoDB table is configured with Auto Scaling so this is not likely to be the bottleneck in order processing.

INCORRECT: "Add an Amazon CloudFront distribution with a custom origin to cache the responses for the web tier" is incorrect. This will cache media files to speed up web response times but not order processing times as they take place in the middle tier.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 29

A company uses Docker containers for many application workloads in an on-premise data center. The company is planning to deploy containers to AWS and the chief architect has mandated that the same configuration and administrative tools must be used across all containerized environments. The company also wishes to remain cloud agnostic to safeguard mitigate the impact of future changes in cloud strategy.

How can a Solutions Architect design a managed solution that will align with open-source software?

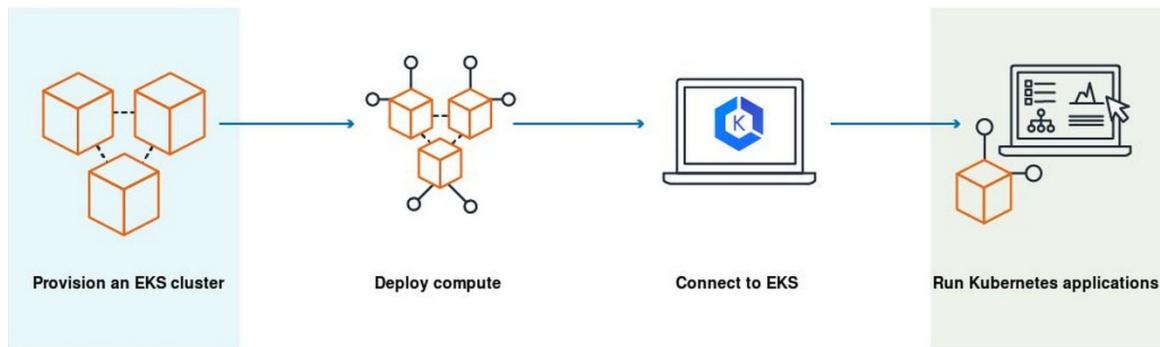
1. Launch the containers on Amazon Elastic Kubernetes Service (EKS) and EKS worker nodes.
2. Launch the containers on a fleet of Amazon EC2 instances in a cluster placement group.
3. Launch the containers on Amazon Elastic Container Service (ECS) with AWS Fargate instances.
4. Launch the containers on Amazon Elastic Container Service (ECS) with Amazon EC2 instance worker nodes.

Answer: 1

Explanation:

Amazon EKS is a managed service that can be used to run Kubernetes on AWS. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications. Applications running on Amazon EKS are fully compatible with applications running on any standard Kubernetes environment, whether running in on-premises data centers or public clouds. This means that you can easily migrate any standard Kubernetes application to Amazon EKS without any code modification.

This solution ensures that the same open-source software is used for automating the deployment, scaling, and management of containerized applications both on-premises and in the AWS Cloud.



CORRECT: "Launch the containers on Amazon Elastic Kubernetes Service (EKS) and EKS worker nodes" is the correct answer.

INCORRECT: "Launch the containers on a fleet of Amazon EC2 instances in a cluster placement group" is incorrect

INCORRECT: "Launch the containers on Amazon Elastic Container Service (ECS) with AWS Fargate instances" is incorrect

INCORRECT: "Launch the containers on Amazon Elastic Container Service (ECS) with Amazon EC2 instance worker nodes" is incorrect

References:

<https://docs.aws.amazon.com/eks/latest/userguide/what-is-eks.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

QUESTION 30

A company has uploaded some highly critical data to an Amazon S3 bucket. Management are concerned about data availability and require that steps are taken to protect the data from accidental deletion. The data should still be accessible, and a user should be able to delete the data intentionally.

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

1. Enable versioning on the S3 bucket.
2. Enable MFA Delete on the S3 bucket.
3. Create a bucket policy on the S3 bucket.
4. Enable default encryption on the S3 bucket.
5. Create a lifecycle policy for the objects in the S3 bucket.

Answer: 1, 2

Explanation:

Multi-factor authentication (MFA) delete adds an additional step before an object can be deleted from a versioning-enabled bucket.

With MFA delete the bucket owner must include the x-amz-mfa request header in requests to permanently delete an object version or change the versioning state of the bucket.

CORRECT: "Enable versioning on the S3 bucket" is a correct answer.

CORRECT: "Enable MFA Delete on the S3 bucket" is also a correct answer.

INCORRECT: "Create a bucket policy on the S3 bucket" is incorrect. A bucket policy is not required to enable MFA delete.

INCORRECT: "Enable default encryption on the S3 bucket" is incorrect. Encryption does protect against deletion.

INCORRECT: "Create a lifecycle policy for the objects in the S3 bucket" is incorrect. A lifecycle policy will move data to another storage class but does not protect against deletion.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 31

A company runs a large batch processing job at the end of every quarter. The processing job runs for 5 days and uses 15 Amazon EC2 instances. The processing must run uninterrupted for 5 hours per day. The company is investigating ways to reduce the cost of the batch processing job.

Which pricing model should the company choose?

1. Reserved Instances
2. Spot Instances
3. On-Demand Instances
4. Dedicated Instances

Answer: 3

Explanation:

Each EC2 instance runs for 5 hours a day for 5 days per quarter or 20 days per year. This is time duration is insufficient to warrant reserved instances as these require a commitment of a minimum of 1 year and the discounts would not outweigh the costs of having the reservations unused for a large percentage of time. In this case, there are no options presented that can reduce the cost and therefore on-demand instances should be used.

CORRECT: "On-Demand Instances" is the correct answer.

INCORRECT: "Reserved Instances" is incorrect. Reserved instances are good for continuously running workloads that run for a period of 1 or 3 years.

INCORRECT: "Spot Instances" is incorrect. Spot instances may be interrupted, and this is not acceptable. Note that Spot Block is deprecated and unavailable to new customers.

INCORRECT: "Dedicated Instances" is incorrect. These do not provide any cost advantages and will be more expensive.

References:

<https://aws.amazon.com/ec2/pricing/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 32

An application is being created that will use Amazon EC2 instances to generate and store data. Another set of EC2 instances will then analyze and modify the data. Storage requirements will be significant and will continue to grow over time. The application architects require a storage solution.

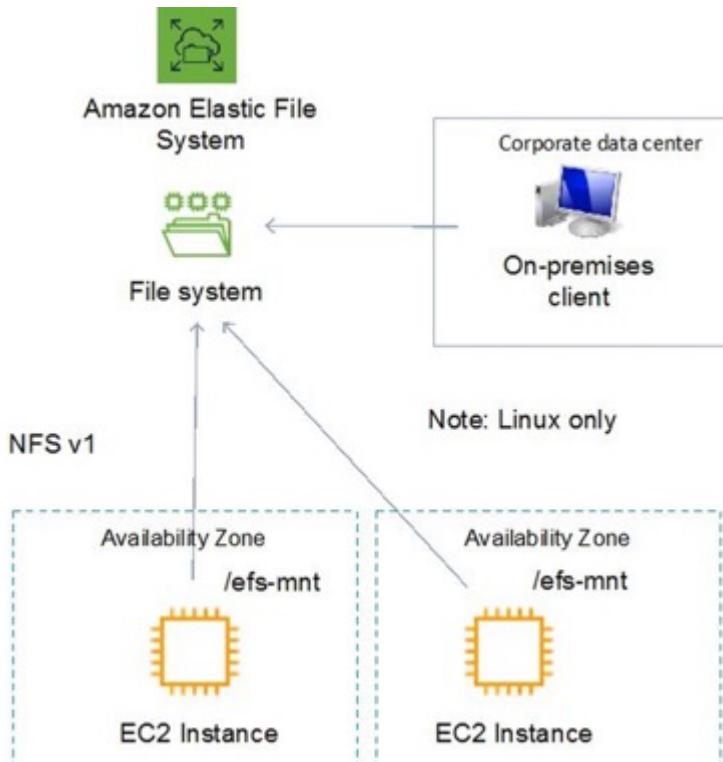
Which actions would meet these needs?

1. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances
2. Store the data in an Amazon EFS filesystem. Mount the file system on the application instances
3. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances
4. Store the data in AWS Storage Gateway. Setup AWS Direct Connect between the Gateway appliance and the EC2 instances

Answer: 2

Explanation:

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.



Amazon EFS supports the Network File System version 4 (NFSv4.1 and NFSv4.0) protocol. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, providing a common data source for workloads and applications running on more than one instance or server.

For this scenario, EFS is a great choice as it will provide a scalable file system that can be mounted by multiple EC2 instances and accessed simultaneously.

CORRECT: "Store the data in an Amazon EFS filesystem. Mount the file system on the application instances" is the correct answer.

INCORRECT: "Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances" is incorrect. Though there is a new feature that allows (EBS multi-attach) that allows attaching multiple Nitro instances to a volume, this is not on the exam yet, and has some specific constraints.

INCORRECT: "Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances" is incorrect as S3 Glacier is not a suitable storage location for live access to data, it is used for archival.

INCORRECT: "Store the data in AWS Storage Gateway. Setup AWS Direct Connect between the Gateway appliance and the EC2 instances" is incorrect. There is no reason to store the data on-premises in a Storage Gateway, using EFS is a much better solution.

References:

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 33

A company hosts a multiplayer game on AWS. The application uses Amazon EC2 instances in a single Availability Zone and users connect over Layer 4. Solutions Architect has been tasked with making the architecture highly available and also more cost-effective.

How can the solutions architect best meet these requirements? (Select TWO.)

1. Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically
2. Increase the number of instances and use smaller EC2 instance types
3. Configure a Network Load Balancer in front of the EC2 instances
4. Configure an Application Load Balancer in front of the EC2 instances
5. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically

Answer: 3, 5

Explanation:

The solutions architect must enable high availability for the architecture and ensure it is cost-effective. To enable high availability an Amazon EC2 Auto Scaling group should be created to add and remove instances across multiple availability zones.

In order to distribute the traffic to the instances the architecture should use a Network Load Balancer which operates at Layer 4. This architecture will also be cost-effective as the Auto Scaling group will ensure the right number of instances are running based on demand.

CORRECT: "Configure a Network Load Balancer in front of the EC2 instances" is a correct answer.

CORRECT: "Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically" is also a correct answer.

INCORRECT: "Increase the number of instances and use smaller EC2 instance types" is incorrect as this is not the most cost-effective option. Auto Scaling should be used to maintain the right number of active instances.

INCORRECT: "Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically" is incorrect as this is not highly available as it's a single AZ.

INCORRECT: "Configure an Application Load Balancer in front of the EC2 instances" is incorrect as an ALB operates at Layer 7 rather than Layer 4.

References:

<https://docsaws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 34

A company delivers content to subscribers distributed globally from an application running on AWS. The application uses a fleet of Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to an update in copyright restrictions, it is necessary to block access for specific countries.

What is the EASIEST method to meet this requirement?

1. Modify the ALB security group to deny incoming traffic from blocked countries
2. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
3. Use Amazon CloudFront to serve the application and deny access to blocked countries
4. Use a network ACL to block the IP address ranges associated with the specific countries

Answer: 3

Explanation:

When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following:

- Allow your users to access your content only if they're in one of the countries on a whitelist of approved countries.
- Prevent your users from accessing your content if they're in one of the countries on a blacklist of banned countries.

For example, if a request comes from a country where, for copyright reasons, you are not authorized to distribute your content, you can use CloudFront geo restriction to block the request.

This is the easiest and most effective way to implement a geographic restriction for the delivery of content.

CORRECT: "Use Amazon CloudFront to serve the application and deny access to blocked countries" is the correct answer.

INCORRECT: "Use a Network ACL to block the IP address ranges associated with the specific countries" is incorrect as this would be extremely difficult to manage.

INCORRECT: "Modify the ALB security group to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.

INCORRECT: "Modify the security group for EC2 instances to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 35

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

1. Amazon EFS
2. Amazon FSx
3. Amazon S3
4. AWS Storage Gateway

Answer: 2

Explanation:

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.

Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs).

Additionally, Amazon FSx for Windows File Server supports Distributed File System Replication (DFSR) in both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.

Deployment type	SSD storage	HDD storage	DFS namespaces	DFS replication	Custom DNS name	CA shares
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		Coming soon	✓*
Multi-AZ	✓	✓	✓		Coming soon	✓*

CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems.

INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.

INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.

References:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 36

A website runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) which serves as an origin for an Amazon CloudFront distribution. An AWS WAF is being used to protect against SQL injection attacks. A 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?

1. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address
2. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address
3. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address
4. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Answer: 2

Explanation:

A new version of the AWS Web Application Firewall was released in November 2019. With AWS WAF classic you create "IP match conditions", whereas with AWS WAF (new version) you create "IP set match statements". Look out for wording on the exam.

The IP match condition / IP set match statement inspects the IP address of a web request's origin against a set of IP addresses and address ranges. Use this to allow or block web requests based on the IP addresses that the requests originate from.

AWS WAF supports all IPv4 and IPv6 address ranges. An IP set can hold up to 10,000 IP addresses or IP address ranges to check.

CORRECT: "Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address" is the correct answer.

INCORRECT: "Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address" is incorrect as CloudFront does not sit within a subnet so network ACLs do not apply to it.

INCORRECT: "Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address" is incorrect as the source IP addresses of the data in the EC2 instances' subnets will be the ELB IP addresses.

INCORRECT: "Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address." is incorrect as you cannot create deny rules with security groups.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-waf-and-shield/>

QUESTION 37

A solutions architect is creating a system that will run analytics on financial data for several hours a night, 5 days a week. The analysis is expected to run for the same duration and cannot be interrupted once it is started. The system will be required for a minimum of 1 year.

What should the solutions architect configure to ensure the EC2 instances are available when they are needed?

1. Savings Plans
2. On-Demand Instances
3. Regional Reserved Instances
4. On-Demand Capacity Reservations

Answer: 4

Explanation:

On-Demand Capacity Reservations enable you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration. This gives you the ability to create and manage Capacity Reservations independently from the billing discounts offered by Savings Plans or Regional Reserved Instances.

By creating Capacity Reservations, you ensure that you always have access to EC2 capacity when you need it, for as long as you need it. You can create Capacity Reservations at any time, without entering a one-year or three-year term commitment, and the capacity is available immediately.

The table below shows the difference between capacity reservations and other options:

	Capacity Reservations	Zonal Reserved Instances	Regional Reserved Instances	Savings Plans
Term	No commitment required. Can be created and canceled as needed.	Requires a fixed one-year or three-year commitment		
Capacity benefit	Capacity reserved in a specific Availability Zone.		No capacity reserved.	
Billing discount	No billing discount. †	Provides a billing discount.		
Instance Limits	Your On-Demand Instance limits per Region apply.	Default is 20 per Availability Zone. You can request a limit increase.	Default is 20 per Region. You can request a limit increase.	No limit.

CORRECT: "On-Demand Capacity Reservations" is the correct answer.

INCORRECT: "Regional Reserved Instances" is incorrect. This type of reservation does not reserve capacity.

INCORRECT: "On-Demand Instances" is incorrect. This does not provide any kind of capacity reservation.

INCORRECT: "Savings Plans" is incorrect. This pricing option does not provide a capacity reservation.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 38

A solutions architect needs to backup some application log files from an online ecommerce store to Amazon S3. It is unknown how often the logs will be accessed or which logs will be accessed the most. The solutions architect must keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

1. S3 Glacier
2. S3 Intelligent-Tiering
3. S3 Standard-Infrequent Access (S3 Standard-IA)
4. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: 2

Explanation:

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead.

It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. This is an ideal use case for intelligent-tiering as the access patterns for the log files are not known.

CORRECT: "S3 Intelligent-Tiering" is the correct answer.

INCORRECT: "S3 Standard-Infrequent Access (S3 Standard-IA)" is incorrect as if the data is accessed often retrieval fees could

become expensive.

INCORRECT: "S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive.

INCORRECT: "S3 Glacier" is incorrect as if the data is accessed often retrieval fees could become expensive. Glacier also requires more work in retrieving the data from the archive and quick access requirements can add further costs.

References:

https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 39

A solutions architect is designing a new service that will use an Amazon API Gateway API on the frontend. The service will need to persist data in a backend database using key-value requests. Initially, the data requirements will be around 1 GB and future growth is unknown. Requests can range from 0 to over 800 requests per second.

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

1. AWS Fargate
2. AWS Lambda
3. Amazon DynamoDB
4. Amazon EC2 Auto Scaling
5. Amazon RDS

Answer: 2, 3

Explanation:

In this case AWS Lambda can perform the computation and store the data in an Amazon DynamoDB table. Lambda can scale concurrent executions to meet demand easily and DynamoDB is built for key-value data storage requirements and is also serverless and easily scalable. This is therefore a cost effective solution for unpredictable workloads.

CORRECT: "AWS Lambda" is a correct answer.

CORRECT: "Amazon DynamoDB" is also a correct answer.

INCORRECT: "AWS Fargate" is incorrect as containers run constantly and therefore incur costs even when no requests are being made.

INCORRECT: "Amazon EC2 Auto Scaling" is incorrect as this uses EC2 instances which will incur costs even when no requests are being made.

INCORRECT: "Amazon RDS" is incorrect as this is a relational database not a No-SQL database. It is therefore not suitable for key-value data storage requirements.

References:

<https://aws.amazon.com/lambda/features/>

<https://aws.amazon.com/dynamodb/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

QUESTION 40

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.)

1. Detach a volume on an EC2 instance and copy it to an Amazon S3 bucket in the second Region
2. Launch a new EC2 instance from an Amazon Machine Image (AMI) in the second Region
3. Launch a new EC2 instance in the second Region and copy a volume from Amazon S3 to the new instance

4. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify the second Region for the destination
5. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the second Region using that EBS volume

Answer: 2, 4

Explanation:

You can copy an Amazon Machine Image (AMI) within or across AWS Regions using the AWS Management Console, the AWS Command Line Interface or SDKs, or the Amazon EC2 API, all of which support the `CopyImage` action.

Using the copied AMI the solutions architect would then be able to launch an instance from the same EBS volume in the second Region.

Note: the AMIs are stored on Amazon S3, however you cannot view them in the S3 management console or work with them programmatically using the S3 API.

CORRECT: "Copy an Amazon Machine Image (AMI) of an EC2 instance and specify the second Region for the destination" is a correct answer.

CORRECT: "Launch a new EC2 instance from an Amazon Machine Image (AMI) in the second Region" is also a correct answer.

INCORRECT: "Detach a volume on an EC2 instance and copy it to an Amazon S3 bucket in the second Region" is incorrect. You cannot copy EBS volumes directly from EBS to Amazon S3.

INCORRECT: "Launch a new EC2 instance in the second Region and copy a volume from Amazon S3 to the new instance" is incorrect. You cannot create an EBS volume directly from Amazon S3.

INCORRECT: "Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the second Region using that EBS volume" is incorrect. You cannot create an EBS volume directly from Amazon S3.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 41

A solutions architect is creating a document submission application for a school. The application will use 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 upload and modify the documents.

Which combination of actions should be taken to meet these requirements? (Select TWO.)

1. Set read-only permissions on the bucket
2. Enable versioning on the bucket
3. Attach an IAM policy to the bucket
4. Enable MFA Delete on the bucket
5. Encrypt the bucket using AWS SSE-S3

Answer: 2, 4

Explanation:

None of the options present a good solution for specifying permissions required to write and modify objects so that requirement needs to be taken care of separately. The other requirements are to prevent accidental deletion and the ensure that all versions of the document are available.

The two solutions for these requirements are versioning and MFA delete. Versioning will retain a copy of each version of the document and multi-factor authentication delete (MFA delete) will prevent any accidental deletion as you need to supply a second factor when attempting a delete.

CORRECT: "Enable versioning on the bucket" is a correct answer.

CORRECT: "Enable MFA Delete on the bucket" is also a correct answer.

INCORRECT: "Set read-only permissions on the bucket" is incorrect as this will also prevent any writing to the bucket which is not desired.

INCORRECT: "Attach an IAM policy to the bucket" is incorrect as users need to modify documents which will also allow delete. Therefore, a method must be implemented to just control deletes.

INCORRECT: "Encrypt the bucket using AWS SSE-S3" is incorrect as encryption doesn't stop you from deleting an object.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 42

A solutions architect is designing an application on AWS. The compute layer will run in parallel across EC2 instances. The compute layer should scale based on the number of jobs to be processed. The compute layer 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?

1. Create an Amazon SNS topic to send the jobs that need 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 CPU usage
2. Create an Amazon SQS queue to hold the jobs that need 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 network usage
3. 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
4. Create an Amazon SNS topic to send the jobs that need 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 messages published to the SNS topic

Answer: 3

Explanation:

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 (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.
- **Acceptable backlog per instance:** To calculate your target value, first determine what your application can accept in terms of latency. Then, take the acceptable latency value and divide it by the average time that an EC2 instance takes to process a message.

This solution will scale EC2 instances using Auto Scaling based on the number of jobs waiting in the SQS queue.

CORRECT: "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" is the correct answer.

INCORRECT: "Create an Amazon SQS queue to hold the jobs that need 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 network usage" is incorrect as scaling on network usage does not relate to the number of jobs waiting to be processed.

INCORRECT: "Create an Amazon SNS topic to send the jobs that need 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 CPU usage" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but

is less suitable than SQS for this use case. Scaling on CPU usage is not the best solution as it does not relate to the number of jobs waiting to be processed.

INCORRECT: "Create an Amazon SNS topic to send the jobs that need 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 messages published to the SNS topic" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on the number of notifications in SNS is not possible.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 43

A team are planning to run analytics jobs on log files each day and require a storage solution. The size and number of logs is unknown and data will persist for 24 hours only.

What is the MOST cost-effective solution?

1. Amazon S3 Glacier Deep Archive
2. Amazon S3 Standard
3. Amazon S3 Intelligent-Tiering
4. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: 2

Explanation:

S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object.

CORRECT: "Amazon S3 Standard" is the correct answer.

INCORRECT: "Amazon S3 Intelligent-Tiering" is incorrect as there is an additional fee for using this service and for a short-term requirement it may not be beneficial.

INCORRECT: "Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as this storage class has a minimum capacity charge per object (128 KB) and a per GB retrieval fee.

INCORRECT: "Amazon S3 Glacier Deep Archive" is incorrect as this storage class is used for archiving data. There are retrieval fees and it takes hours to retrieve data from an archive.

References:

<https://aws.amazon.com/s3/storage-classes/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 44

A company runs a web application that serves weather updates. The application runs on a fleet of Amazon EC2 instances in a Multi-AZ Auto scaling group behind an Application Load Balancer (ALB). The instances store data in an Amazon Aurora database. A solutions architect needs to make the application more resilient to sporadic increases in request rates.

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

1. Add and AWS WAF in front of the ALB
2. Add Amazon Aurora Replicas
3. Add an AWS Transit Gateway to the Availability Zones
4. Add an AWS Global Accelerator endpoint
5. Add an Amazon CloudFront distribution in front of the ALB

Answer: 2, 5

Explanation:

The architecture is already highly resilient but may be subject to performance degradation if there are sudden increases in request rates. To resolve this situation Amazon Aurora Read Replicas can be used to serve read traffic which offloads requests from the main database. On the frontend an Amazon CloudFront distribution can be placed in front of the ALB and this will cache content for better performance and also offloads requests from the backend.

CORRECT: "Add Amazon Aurora Replicas" is the correct answer.

CORRECT: "Add an Amazon CloudFront distribution in front of the ALB" is the correct answer.

INCORRECT: "Add an AWS WAF in front of the ALB" is incorrect. A web application firewall protects applications from malicious attacks. It does not improve performance.

INCORRECT: "Add an AWS Transit Gateway to the Availability Zones" is incorrect as this is used to connect on-premises networks to VPCs.

INCORRECT: "Add an AWS Global Accelerator endpoint" is incorrect as this service is used for directing users to different instances of the application in different regions based on latency.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 45

An Amazon VPC contains several Amazon EC2 instances. The instances need to make API calls to Amazon DynamoDB. A solutions architect needs to ensure that the API calls do not traverse the internet.

How can this be accomplished? (Select TWO.)

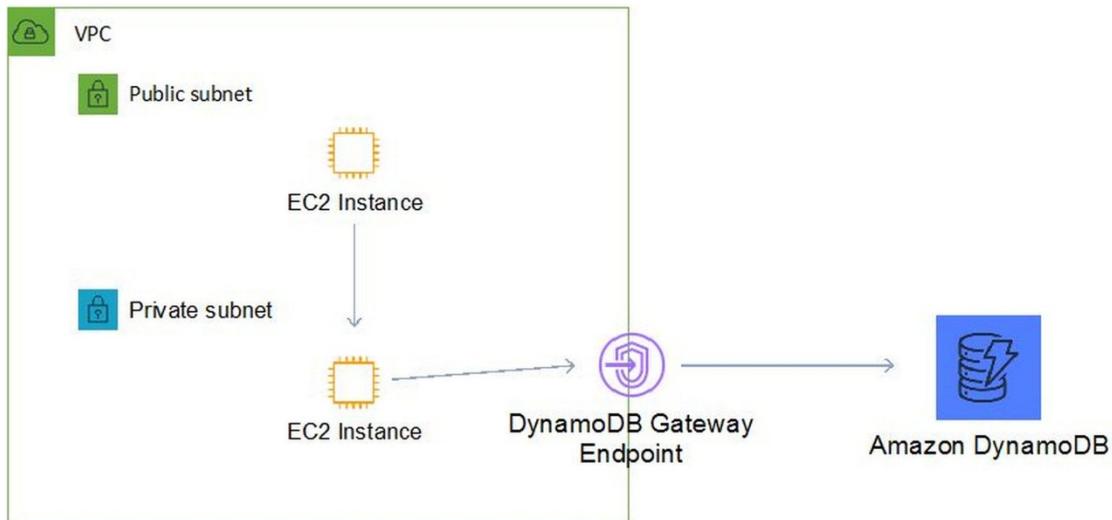
1. Create a route table entry for the endpoint
2. Create a gateway endpoint for DynamoDB
3. Create a new DynamoDB table that uses the endpoint
4. Create an ENI for the endpoint in each of the subnets of the VPC
5. Create a VPC peering connection between the VPC and DynamoDB

Answer: 1, 2

Explanation:

Amazon DynamoDB and Amazon S3 support gateway endpoints, not interface endpoints. With a gateway endpoint you create the endpoint in the VPC, attach a policy allowing access to the service, and then specify the route table to create a route table entry in.

Default VPC



Route Table

Destination	Target
0.0.0.0/0	vpnd

CORRECT: "Create a route table entry for the endpoint" is a correct answer.

CORRECT: "Create a gateway endpoint for DynamoDB" is also a correct answer.

INCORRECT: "Create a new DynamoDB table that uses the endpoint" is incorrect as it is not necessary to create a new DynamoDB table.

INCORRECT: "Create an ENI for the endpoint in each of the subnets of the VPC" is incorrect as an ENI is used by an interface endpoint, not a gateway endpoint.

INCORRECT: "Create a VPC peering connection between the VPC and DynamoDB" is incorrect as you cannot create a VPC peering connection between a VPC and a public AWS service as public services are outside of VPCs.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 46

A solutions architect is designing the infrastructure to run an application on Amazon EC2 instances. The application requires high availability and must dynamically scale based on demand to be cost efficient.

What should the solutions architect do to meet these requirements?

1. Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Regions
2. Configure an Amazon CloudFront distribution in front of an Auto Scaling group to deploy instances to multiple Regions
3. Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Availability Zones
4. Configure an Amazon API Gateway API in front of an Auto Scaling group to deploy instances to multiple Availability Zones

Answer: 3**Explanation:**

The Amazon EC2-based application must be highly available and elastically scalable. Auto Scaling can provide the elasticity by dynamically launching and terminating instances based on demand. This can take place across availability zones for high availability.

Incoming connections can be distributed to the instances by using an Application Load Balancer (ALB).

CORRECT: "Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Availability Zones" is the correct answer.

INCORRECT: "Configure an Amazon API Gateway API in front of an Auto Scaling group to deploy instances to multiple Availability Zones" is incorrect as API gateway is not used for load balancing connections to Amazon EC2 instances.

INCORRECT: "Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Regions" is incorrect as you cannot launch instances in multiple Regions from a single Auto Scaling group.

INCORRECT: "Configure an Amazon CloudFront distribution in front of an Auto Scaling group to deploy instances to multiple Regions" is incorrect as you cannot launch instances in multiple Regions from a single Auto Scaling group.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html>

<https://aws.amazon.com/elasticloadbalancing/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 47

A retail company with many stores and warehouses is implementing IoT sensors to gather monitoring data from devices in each location. The data will be sent to AWS in real time. A solutions architect must provide a solution for ensuring events are received in order for each device and ensure that data is saved for future processing.

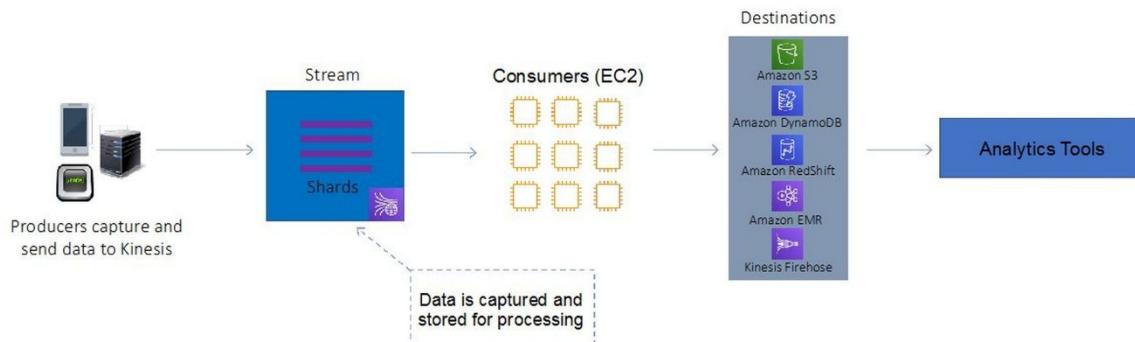
Which solution would be MOST efficient?

1. Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3
2. Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS
3. Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS
4. Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3

Answer: 1**Explanation:**

Amazon Kinesis Data Streams collect and process data in real time. A *Kinesis data stream* is a set of [shards](#). Each shard has a sequence of data records. Each data record has a [sequence number](#) that is assigned by Kinesis Data Streams. A *shard* is a uniquely identified sequence of data records in a stream.

A *partition key* is used to group data by shard within a stream. Kinesis Data Streams segregates the data records belonging to a stream into multiple shards. It uses the partition key that is associated with each data record to determine which shard a given data record belongs to.



For this scenario, the solutions architect can use a partition key for each device. This will ensure the records for that device are grouped by shard and the shard will ensure ordering. Amazon S3 is a valid destination for saving the data records.

CORRECT: "Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3" is the correct answer.

INCORRECT: "Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS" is incorrect as you cannot save data to EBS from Kinesis.

INCORRECT: "Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS" is incorrect as SQS is not the most efficient service for streaming, real time data.

INCORRECT: "Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3" is incorrect as SQS is not the most efficient service for streaming, real time data.

References:

<https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>

QUESTION 48

An organization want to share regular updates about their charitable work using static webpages. The pages are expected to generate a large amount of views from 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?

1. Generate presigned URLs for the files
2. Use cross-Region replication to all Regions
3. Use the geoproximity feature of Amazon Route 53
4. Use Amazon CloudFront with the S3 bucket as its origin

Answer: 4

Explanation:

Amazon CloudFront can be used to cache the files in edge locations around the world and this will improve the performance of the webpages.

To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:

- Using a REST API endpoint as the origin with access restricted by an [origin access identity \(OAI\)](#)
- Using a website endpoint as the origin with anonymous (public) access allowed
- Using a website endpoint as the origin with access restricted by a Referer header

CORRECT: "Use Amazon CloudFront with the S3 bucket as its origin" is the correct answer.

INCORRECT: "Generate presigned URLs for the files" is incorrect as this is used to restrict access which is not a requirement.

INCORRECT: "Use cross-Region replication to all Regions" is incorrect as this does not provide a mechanism for directing users to the closest copy of the static webpages.

INCORRECT: "Use the geoproximity feature of Amazon Route 53" is incorrect as this does not include a solution for having multiple copies of the data in different geographic locations.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 49

An insurance company has a web application that serves users in the United Kingdom and Australia. The application includes a database tier using a MySQL database hosted in eu-west-2. The web tier runs from eu-west-2 and ap-southeast-2. Amazon Route 53 geoproximity routing is used to direct users to the closest web tier. It has been noted that Australian users receive slow response times to queries.

Which changes should be made to the database tier to improve performance?

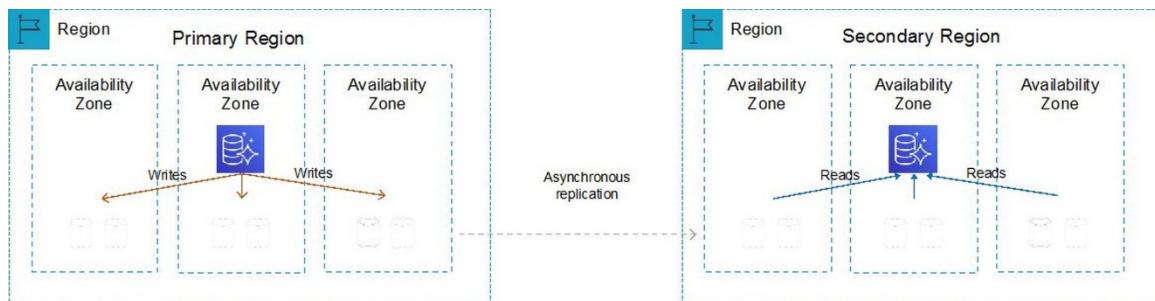
1. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region
2. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions
3. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance
4. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2

Answer: 4

Explanation:

The issue here is latency with read queries being directed from Australia to UK which is great physical distance. A solution is required for improving read performance in Australia.

An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only, secondary AWS Regions. Aurora replicates data to the secondary AWS Regions with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS Region.



Aurora Global Database:

- Uses physical replication
- One secondary AWS region
- Uses dedicated infrastructure
- No impact on DB performance
- Good for disaster recovery

This solution will provide better performance for users in the Australia Region for queries. Writes must still take place in the UK Region but read performance will be greatly improved.

CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2" is the correct answer.

INCORRECT: "Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region" is incorrect. The database is located in UK. If the database is migrated to Australia then the reverse problem will occur. Multi-AZ does not assist with improving query performance across Regions.

INCORRECT: "Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions" is incorrect as a relational database running on MySQL is unlikely to be compatible with DynamoDB.

INCORRECT: "Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance" is incorrect as you can only put ALBs in front of the web tier, not the DB tier.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>

QUESTION 50

A web application runs in public and private subnets. The application architecture consists of a web tier and database tier running on Amazon EC2 instances. Both tiers run in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

1. Create new public and private subnets in the same AZ for high availability
2. Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs
3. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)
4. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ
5. Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment

Answer: 2, 5

Explanation:

To add high availability to this architecture both the web tier and database tier require changes. For the web tier an Auto Scaling group across multiple AZs with an ALB will ensure there are always instances running and traffic is being distributed to them.

The database tier should be migrated from the EC2 instances to Amazon RDS to take advantage of a managed database with Multi-AZ functionality. This will ensure that if there is an issue preventing access to the primary database a secondary database can take over.

CORRECT: "Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs" is the correct answer.

CORRECT: "Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment" is the correct answer.

INCORRECT: "Create new public and private subnets in the same AZ for high availability" is incorrect as this would not add high availability.

INCORRECT: "Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)" is incorrect because the existing servers are in a single subnet. For HA we need to instances in multiple subnets.

INCORRECT: "Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ" is incorrect because we also need HA for the database layer.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>

<https://aws.amazon.com/rds/features/multi-az/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 51

An application running on an Amazon ECS container instance using the EC2 launch type needs permissions to write data to Amazon DynamoDB.

How can you assign these permissions only to the specific ECS task that is running the application?

1. Create an IAM policy with permissions to DynamoDB and attach it to the container instance
2. Create an IAM policy with permissions to DynamoDB and assign it to a task using the *taskRoleArn* parameter
3. Use a security group to allow outbound connections to DynamoDB and assign it to the container instance
4. Modify the *AmazonECSTaskExecutionRolePolicy* policy to add permissions for DynamoDB

Answer: 2

Explanation:

To specify permissions for a specific task on Amazon ECS you should use IAM Roles for Tasks. The permissions policy can be applied to tasks when creating the task definition, or by using an IAM task role override using the AWS CLI or SDKs. The *taskRoleArn* parameter is used to specify the policy.

CORRECT: "Create an IAM policy with permissions to DynamoDB and assign it to a task using the *taskRoleArn* parameter" is the correct answer.

INCORRECT: "Create an IAM policy with permissions to DynamoDB and attach it to the container instance" is incorrect. You should not apply the permissions to the container instance as they will then apply to all tasks running on the instance as well as the instance itself.

INCORRECT: "Use a security group to allow outbound connections to DynamoDB and assign it to the container instance" is incorrect. Though you will need a security group to allow outbound connections to DynamoDB, the question is asking how to assign permissions to write data to DynamoDB and a security group cannot provide those permissions.

INCORRECT: "Modify the *AmazonECSTaskExecutionRolePolicy* policy to add permissions for DynamoDB" is incorrect. The *AmazonECSTaskExecutionRolePolicy* policy is the Task Execution IAM Role. This is used by the container agent to be able to pull container images, write log file etc.

References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

QUESTION 52

An organization has a large amount of data on Windows (SMB) file shares in their on-premises data center. The organization would like to move data into Amazon S3. They would like to automate the migration of data over their AWS Direct Connect link.

Which AWS service can assist them?

1. AWS Database Migration Service (DMS)
2. AWS CloudFormation
3. AWS Snowball
4. AWS DataSync

Answer: 4

Explanation:

AWS DataSync can be used to move large amounts of data online between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS). DataSync eliminates or automatically handles many of these tasks, including scripting copy jobs, scheduling and monitoring transfers, validating data, and optimizing network utilization. The source datastore can be Server Message Block (SMB) file servers.

CORRECT: "AWS DataSync" is the correct answer.

INCORRECT: "AWS Database Migration Service (DMS)" is incorrect. AWS Database Migration Service (DMS) is used for migrating databases, not data on file shares.

INCORRECT: "AWS CloudFormation" is incorrect. AWS CloudFormation can be used for automating infrastructure provisioning.

This is not the best use case for CloudFormation as DataSync is designed specifically for this scenario.

INCORRECT: "AWS Snowball" is incorrect. AWS Snowball is a hardware device that is used for migrating data into AWS. The organization plan to use their Direct Connect link for migrating data rather than sending it in via a physical device. Also, Snowball will not automate the migration.

References:

<https://aws.amazon.com/datasync/faqs/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-datasync/>

QUESTION 53

The database tier of a web application is running on a Windows server on-premises. The database is a Microsoft SQL Server database. The application owner would like to migrate the database to an Amazon RDS instance.

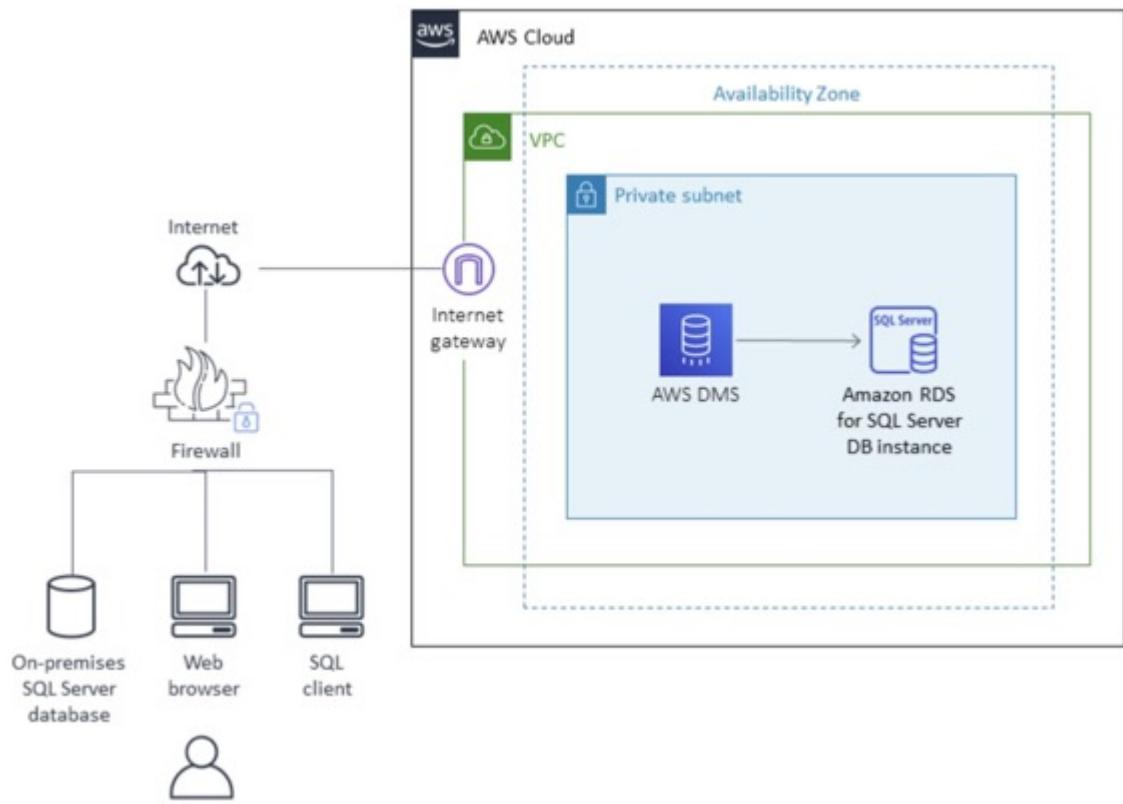
How can the migration be executed with minimal administrative effort and downtime?

1. Use the AWS Server Migration Service (SMS) to migrate the server to Amazon EC2. Use AWS Database Migration Service (DMS) to migrate the database to RDS
2. Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS
3. Use AWS DataSync to migrate the data from the database to Amazon S3. Use AWS Database Migration Service (DMS) to migrate the database to RDS
4. Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS. Use the Schema Conversion Tool (SCT) to enable conversion from Microsoft SQL Server to Amazon RDS

Answer: 2

Explanation:

You can directly migrate Microsoft SQL Server from an on-premises server into Amazon RDS using the Microsoft SQL Server database engine. This can be achieved using the native Microsoft SQL Server tools, or using AWS DMS as depicted below:



CORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS" is the correct answer.

INCORRECT: "Use the AWS Server Migration Service (SMS) to migrate the server to Amazon EC2. Use AWS Database Migration Service (DMS) to migrate the database to RDS" is incorrect. You do not need to use the AWS SMS service to migrate the server into EC2 first. You can directly migrate the database online with minimal downtime.

INCORRECT: "Use AWS DataSync to migrate the data from the database to Amazon S3. Use AWS Database Migration Service (DMS) to migrate the database to RDS" is incorrect. AWS DataSync is used for migrating data, not databases.

INCORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS. Use the Schema Conversion Tool (SCT) to enable conversion from Microsoft SQL Server to Amazon RDS" is incorrect. You do not need to use the SCT as you are migrating into the same destination database engine (RDS is just the platform).

References:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-microsoft-sql-server-database-to-amazon-rds-for-sql-server.html>

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Source.html

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.html

<https://aws.amazon.com/dms/schema-conversion-tool/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-database-migration-service/>

QUESTION 54

A new application will run across multiple Amazon ECS tasks. Front-end application logic will process data and then pass that data to a back-end ECS task to perform further processing and write the data to a datastore. The Architect would like to reduce-

interdependencies so failures do no impact other components.

Which solution should the Architect use?

1. Create an Amazon Kinesis Firehose delivery stream and configure the front-end to add data to the stream and the back-end to read data from the stream
2. Create an Amazon Kinesis Firehose delivery stream that delivers data to an Amazon S3 bucket, configure the front-end to write data to the stream and the back-end to read data from Amazon S3
3. Create an Amazon SQS queue that pushes messages to the back-end. Configure the front-end to add messages to the queue
4. Create an Amazon SQS queue and configure the front-end to add messages to the queue and the back-end to poll the queue for messages

Answer: 4

Explanation:

This is a good use case for Amazon SQS. SQS is a service that is used for decoupling applications, thus reducing interdependencies, through a message bus. The front-end application can place messages on the queue and the back-end can then poll the queue for new messages. Please remember that Amazon SQS is pull-based (polling) not push-based (use SNS for push-based).

CORRECT: "Create an Amazon SQS queue and configure the front-end to add messages to the queue and the back-end to poll the queue for messages" is the correct answer.

INCORRECT: "Create an Amazon Kinesis Firehose delivery stream and configure the front-end to add data to the stream and the back-end to read data from the stream" is incorrect. Amazon Kinesis Firehose is used for streaming data. With Firehose the data is immediately loaded into a destination that can be Amazon S3, RedShift, Elasticsearch, or Splunk. This is not an ideal use case for Firehose as this is not streaming data and there is no need to load data into an additional AWS service.

INCORRECT: "Create an Amazon Kinesis Firehose delivery stream that delivers data to an Amazon S3 bucket, configure the front-end to write data to the stream and the back-end to read data from Amazon S3" is incorrect as per the previous explanation.

INCORRECT: "Create an Amazon SQS queue that pushes messages to the back-end. Configure the front-end to add messages to the queue" is incorrect as SQS is pull-based, not push-based. EC2 instances must poll the queue to find jobs to process.

References:

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/common_use_cases.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 55

Amazon EC2 instances in a development environment run between 9am and 5pm Monday-Friday. Production instances run 24/7. Which pricing models should be used to optimize cost and ensure capacity is available? (Select TWO.)

1. Use Spot instances for the development environment
2. Use Reserved instances for the development environment
3. On-demand capacity reservations for the development environment
4. Use Reserved instances for the production environment
5. Use On-Demand instances for the production environment

Answer: 3,4

Explanation:

Capacity reservations have no commitment and can be created and canceled as needed. This is ideal for the development environment as it will ensure the capacity is available. There is no price advantage but none of the other options provide a price advantage whilst also ensuring capacity is available

Reserved instances are a good choice for workloads that run continuously. This is a good option for the production environment.

CORRECT: "On-demand capacity reservations for the development environment" is a correct answer.

CORRECT: "Use Reserved instances for the production environment" is also a correct answer.

INCORRECT: "Use Spot instances for the development environment" is incorrect. Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. Spot instances are not suitable for the development environment as important work may be interrupted.

INCORRECT: "Use Reserved instances for the development environment" is incorrect as they require a long-term commitment which is not ideal for a development environment.

INCORRECT: "Use On-Demand instances for the production environment" is incorrect. There is no long-term commitment required when you purchase On-Demand Instances. However, you do not get any discount and therefore this is the most expensive option.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/instance-purchasing-options.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 56

An application running on Amazon EC2 needs to asynchronously invoke an AWS Lambda function to perform data processing. The services should be decoupled.

Which service can be used to decouple the compute services?

1. AWS Config
2. Amazon SNS
3. Amazon MQ
4. AWS Step Functions

Answer: 2

Explanation:

You can use a Lambda function to process Amazon Simple Notification Service notifications. Amazon SNS supports Lambda functions as a target for messages sent to a topic. This solution decouples the Amazon EC2 application from Lambda and ensures the Lambda function is invoked.

CORRECT: "Amazon SNS" is the correct answer.

INCORRECT: "AWS Config" is incorrect. AWS Config is a service that is used for continuous compliance, not application decoupling.

INCORRECT: "Amazon MQ" is incorrect. Amazon MQ is similar to SQS but is used for existing applications that are being migrated into AWS. SQS should be used for new applications being created in the cloud.

INCORRECT: "AWS Step Functions" is incorrect. AWS Step Functions is a workflow service. It is not the best solution for this scenario.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html>

<https://aws.amazon.com/sns/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/>

QUESTION 57

A company wishes to restrict access to their Amazon DynamoDB table to specific, private source IP addresses from their VPC. What should be done to secure access to the table?

1. Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)
2. Create a gateway VPC endpoint and add an entry to the route table

3. Create the Amazon DynamoDB table in the VPC
4. Create an AWS VPN connection to the Amazon DynamoDB endpoint

Answer: 2

Explanation:

There are two different types of VPC endpoint: interface endpoint, and gateway endpoint. With an interface endpoint you use an ENI in the VPC. With a gateway endpoint you configure your route table to point to the endpoint. Amazon S3 and DynamoDB use gateway endpoints. This solution means that all traffic will go through the VPC endpoint straight to DynamoDB using private IP addresses.

		Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route	
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic	
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB	
Security	Security Groups	VPC Endpoint Policies	

CORRECT: "Create a gateway VPC endpoint and add an entry to the route table" is the correct answer.

INCORRECT: "Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)" is incorrect. As mentioned above, an interface endpoint is not used for DynamoDB, you must use a gateway endpoint.

INCORRECT: "Create the Amazon DynamoDB table in the VPC" is incorrect. You cannot create a DynamoDB table in a VPC, to connect securely using private addresses you should use a gateway endpoint instead.

INCORRECT: "Create an AWS VPN connection to the Amazon DynamoDB endpoint" is incorrect. You cannot create an AWS VPN connection to the Amazon DynamoDB endpoint.

References:

https://docs.amazonaws.cn/en_us/vpc/latest/userguide/vpc-endpoints-ddb.html

<https://aws.amazon.com/premiumsupport/knowledge-center/iam-restrict-calls-ip-addresses/>

<https://aws.amazon.com/blogs/aws/new-vpc-endpoints-for-dynamodb/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 58

An AWS Organization has an OU with multiple member accounts in it. The company needs to restrict the ability to launch only specific Amazon EC2 instance types. How can this policy be applied across the accounts with the least effort?

1. Create an SCP with an allow rule that allows launching the specific instance types
2. Create an SCP with a deny rule that denies all but the specific instance types
3. Create an IAM policy to deny launching all but the specific instance types
4. Use AWS Resource Access Manager to control which launch types can be used

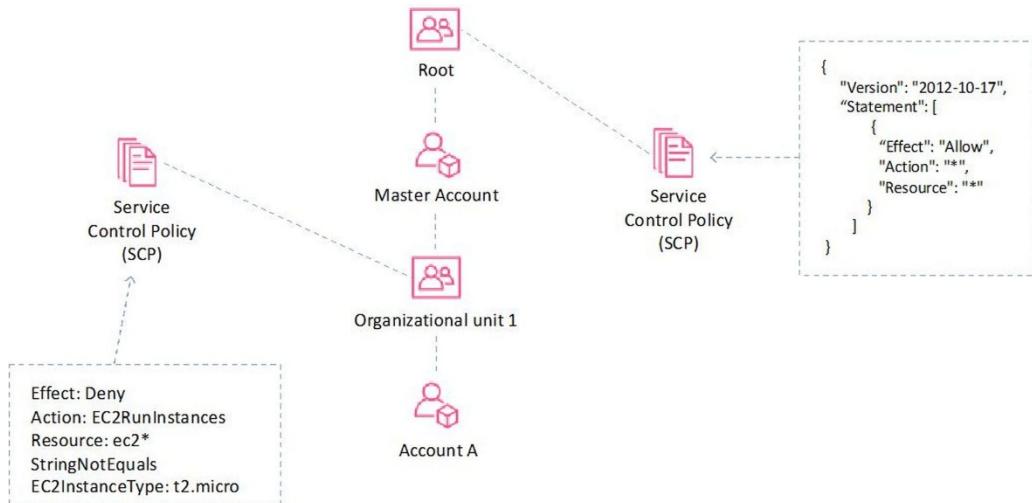
Answer: 2

Explanation:

To apply the restrictions across multiple member accounts you must use a Service Control Policy (SCP) in the AWS Organization.

The way you would do this is to create a deny rule that applies to anything that does not equal the specific instance type you want to allow.

The following architecture could be used to achieve this goal:



CORRECT: "Create an SCP with a deny rule that denies all but the specific instance types" is the correct answer.

INCORRECT: "Create an SCP with an allow rule that allows launching the specific instance types" is incorrect as a deny rule is required.

INCORRECT: "Create an IAM policy to deny launching all but the specific instance types" is incorrect. With IAM you need to apply the policy within each account rather than centrally so this would require much more effort.

INCORRECT: "Use AWS Resource Access Manager to control which launch types can be used" is incorrect. AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. It is not used for restricting access or permissions.

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html#example-ec2-instances

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-organizations/>

QUESTION 59

An Amazon RDS Read Replica is being deployed in a separate region. The master database is not encrypted but all data in the new region must be encrypted. How can this be achieved?

1. Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica
2. Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot
3. Enabled encryption on the master DB instance, then create an encrypted cross-region Read Replica
4. Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica

Answer: 4

Explanation:

You cannot create an encrypted Read Replica from an unencrypted master DB instance. You also cannot enable encryption after launch time for the master DB instance. Therefore, you must create a new master DB by taking a snapshot of the existing DB, encrypting it, and then creating the new DB from the snapshot. You can then create the encrypted cross-region Read Replica of the master DB.

CORRECT: "Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica" is the correct answer.

INCORRECT: "Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica" is incorrect. All other options will not work due to the limitations explained above.

INCORRECT: "Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot" is incorrect. All other options will not work due to the limitations explained above.

INCORRECT: "Enabled encryption on the master DB instance, then create an encrypted cross-region Read Replica" is incorrect. All other options will not work due to the limitations explained above.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 60

A legacy tightly-coupled High Performance Computing (HPC) application will be migrated to AWS. Which network adapter type should be used?

1. Elastic Network Interface (ENI)
2. Elastic Network Adapter (ENA)
3. Elastic Fabric Adapter (EFA)
4. Elastic IP Address

Answer: 3

Explanation:

An Elastic Fabric Adapter is an AWS Elastic Network Adapter (ENA) with added capabilities. The EFA lets you apply the scale, flexibility, and elasticity of the AWS Cloud to tightly-coupled HPC apps. It is ideal for tightly coupled app as it uses the Message Passing Interface (MPI).

CORRECT: "Elastic Fabric Adapter (EFA)" is the correct answer.

INCORRECT: "Elastic Network Interface (ENI)" is incorrect. The ENI is a basic type of adapter and is not the best choice for this use case.

INCORRECT: "Elastic Network Adapter (ENA)" is incorrect. The ENA, which provides Enhanced Networking, does provide high bandwidth and low inter-instance latency but it does not support the features for a tightly-coupled app that the EFA does.

INCORRECT: "Elastic IP Address" is incorrect. An Elastic IP address is just a static public IP address, it is not a type of network adapter.

References:

<https://aws.amazon.com/blogs/aws/now-available-elastic-fabric-adapter-efa-for-tightly-coupled-hpc-workloads/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 61

A new application is to be published in multiple regions around the world. The Architect needs to ensure only 2 IP addresses need to be whitelisted. The solution should intelligently route traffic for lowest latency and provide fast regional failover.

How can this be achieved?

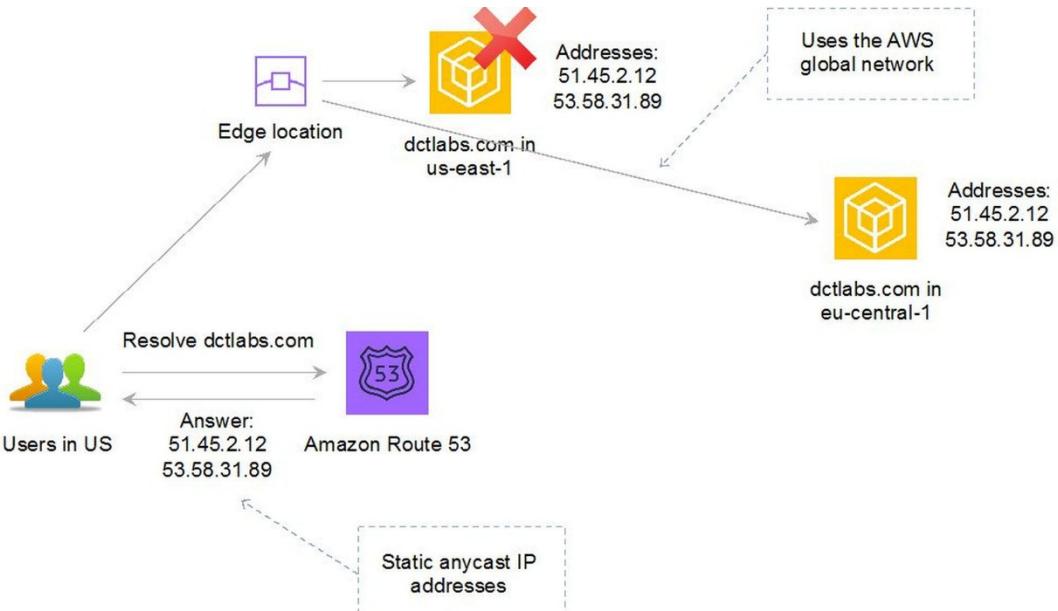
1. Launch EC2 instances into multiple regions behind an NLB with a static IP address
2. Launch EC2 instances into multiple regions behind an ALB and use a Route 53 failover routing policy
3. Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator
4. Launch EC2 instances into multiple regions behind an ALB and use Amazon CloudFront with a pair of static IP addresses

Answer: 3

Explanation:

AWS Global Accelerator uses the vast, congestion-free AWS global network to route TCP and UDP traffic to a healthy application endpoint in the closest AWS Region to the user.

This means it will intelligently route traffic to the closest point of presence (reducing latency). Seamless failover is ensured as AWS Global Accelerator uses anycast IP address which means the IP does not change when failing over between regions so there are no issues with client caches having incorrect entries that need to expire.



This is the only solution that provides deterministic failover.

CORRECT: "Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator" is the correct answer.

INCORRECT: "Launch EC2 instances into multiple regions behind an NLB with a static IP address" is incorrect. An NLB with a static IP is a workable solution as you could configure a primary and secondary address in applications. However, this solution does not intelligently route traffic for lowest latency.

INCORRECT: "Launch EC2 instances into multiple regions behind an ALB and use a Route 53 failover routing policy" is incorrect. A Route 53 failover routing policy uses a primary and standby configuration. Therefore, it sends all traffic to the primary until it fails a health check at which time it sends traffic to the secondary. This solution does not intelligently route traffic for lowest latency.

INCORRECT: "Launch EC2 instances into multiple regions behind an ALB and use Amazon CloudFront with a pair of static IP addresses" is incorrect. Amazon CloudFront cannot be configured with "a pair of static IP addresses".

References:

<https://aws.amazon.com/global-accelerator/>

<https://aws.amazon.com/global-accelerator/faqs/>

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-global-accelerator/>

QUESTION 62

A manufacturing company captures data from machines running at customer sites. Currently, thousands of machines send data every 5 minutes, and this is expected to grow to hundreds of thousands of machines in the near future. The data is logged with the intent to be analyzed in the future as needed.

What is the SIMPLEST method to store this streaming data at scale?

1. Create an Amazon EC2 instance farm behind an ELB to store the data in Amazon EBS Cold HDD volumes
2. Create an Amazon SQS queue, and have the machines write to the queue
3. Create an Amazon Kinesis Firehose delivery stream to store the data in Amazon S3
4. Create an Auto Scaling Group of Amazon EC2 instances behind ELBs to write data into Amazon RDS

Answer: 3

Explanation:

Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It captures, transforms, and loads streaming data and you can deliver the data to "destinations" including Amazon S3 buckets for later analysis

CORRECT: "Create an Amazon Kinesis Firehose delivery stream to store the data in Amazon S3" is the correct answer.

INCORRECT: "Create an Amazon EC2 instance farm behind an ELB to store the data in Amazon EBS Cold HDD volumes" is incorrect. Storing the data in EBS would be expensive and as EBS volumes cannot be shared by multiple instances you would have a bottleneck of a single EC2 instance writing the data.

INCORRECT: "Create an Amazon SQS queue, and have the machines write to the queue" is incorrect. Using an SQS queue to store the data is not possible as the data needs to be stored long-term and SQS queues have a maximum retention time of 14 days.

INCORRECT: "Create an Auto Scaling Group of Amazon EC2 instances behind ELBs to write data into Amazon RDS" is incorrect. Writing data into RDS via a series of EC2 instances and a load balancer is more complex and more expensive. RDS is also not an ideal data store for this data.

References:

<https://aws.amazon.com/kinesis/data-firehose/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>

QUESTION 63

A recent security audit uncovered some poor deployment and configuration practices within your VPC. You need to ensure that applications are deployed in secure configurations.

How can this be achieved in the most operationally efficient manner?

1. Remove the ability for staff to deploy applications
2. Use CloudFormation with securely configured templates
3. Manually check all application configurations before deployment
4. Use AWS Inspector to apply secure configurations

Answer: 2

Explanation:

CloudFormation helps users to deploy resources in a consistent and orderly way. By ensuring the CloudFormation templates are created and administered with the right security configurations for your resources, you can then repeatedly deploy resources with secure settings and reduce the risk of human error.

CORRECT: "Use CloudFormation with securely configured templates" is the correct answer.

INCORRECT: "Remove the ability for staff to deploy applications" is incorrect. Removing the ability of staff to deploy resources does not help you to deploy applications securely as it does not solve the problem of how to do this in an operationally efficient manner.

INCORRECT: "Manually check all application configurations before deployment" is incorrect. Manual checking of all application configurations before deployment is not operationally efficient.

INCORRECT: "Use AWS Inspector to apply secure configurations" is incorrect. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications **deployed** on AWS. It is not used to secure the actual deployment of resources, only to assess the deployed state of the resources.

References:

<https://aws.amazon.com/cloudformation/resources/templates/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/>

QUESTION 64

An e-commerce application is hosted in AWS. The last time a new product was launched, the application experienced a performance issue due to an enormous spike in traffic. Management decided that capacity must be doubled this week after the product is launched.

What is the MOST efficient way for management to ensure that capacity requirements are met?

1. Add a Step Scaling policy
2. Add a Simple Scaling policy
3. Add a Scheduled Scaling action
4. Add Amazon EC2 Spot instances

Answer: 3

Explanation:

Scaling based on a schedule allows you to set your own scaling schedule for predictable load changes. To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. This is ideal for situations where you know when and for how long you are going to need the additional capacity.

CORRECT: "Add a Scheduled Scaling action" is the correct answer.

INCORRECT: "Add a Step Scaling policy" is incorrect. Step scaling policies increase or decrease the current capacity of your Auto Scaling group based on a set of scaling adjustments, known as step adjustments. The adjustments vary based on the size of the alarm breach. This is more suitable to situations where the load unpredictable.

INCORRECT: "Add a Simple Scaling policy" is incorrect. AWS recommend using step over simple scaling in most cases. With simple scaling, after a scaling activity is started, the policy must wait for the scaling activity or health check replacement to complete and the cooldown period to expire before responding to additional alarms (in contrast to step scaling). Again, this is more suitable to unpredictable workloads.

INCORRECT: "Add Amazon EC2 Spot instances" is incorrect. Adding spot instances may decrease EC2 costs but you still need to ensure they are available. The main requirement of the question is that the performance issues are resolved rather than the cost being minimized.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 65

Your company shares some HR videos stored in an Amazon S3 bucket via CloudFront. You need to restrict access to the private content so users coming from specific IP addresses can access the videos and ensure direct access via the Amazon S3 bucket is not possible.

How can this be achieved?

1. Configure CloudFront to require users to access the files using signed cookies, create an origin access identity (OAI) and instruct users to login with the OAI
2. Configure CloudFront to require users to access the files using a signed URL, create an origin access identity (OAI) and restrict access to the files in the Amazon S3 bucket to the OAI
3. Configure CloudFront to require users to access the files using signed cookies, and move the files to an encrypted EBS volume
4. Configure CloudFront to require users to access the files using a signed URL, and configure the S3 bucket as a website endpoint

Answer: 2

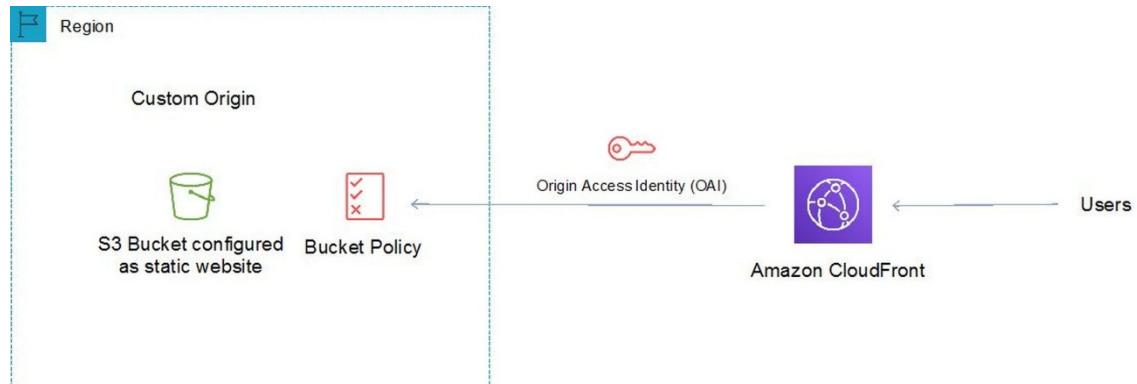
Explanation:

A signed URL includes additional information, for example, an expiration date and time, that gives you more control over access

to your content. You can also specify the IP address or range of IP addresses of the users who can access your content.

If you use CloudFront signed URLs (or signed cookies) to limit access to files in your Amazon S3 bucket, you may also want to prevent users from directly accessing your S3 files by using Amazon S3 URLs. To achieve this you can create an origin access identity (OAI), which is a special CloudFront user, and associate the OAI with your distribution.

You can then change the permissions either on your Amazon S3 bucket or on the files in your bucket so that only the origin access identity has read permission (or read and download permission).



CORRECT: "Configure CloudFront to require users to access the files using a signed URL, create an origin access identity (OAI) and restrict access to the files in the Amazon S3 bucket to the OAI" is the correct answer.

INCORRECT: "Configure CloudFront to require users to access the files using signed cookies, create an origin access identity (OAI) and instruct users to login with the OAI" is incorrect. Users cannot login with an OAI.

INCORRECT: "Configure CloudFront to require users to access the files using signed cookies, and move the files to an encrypted EBS volume" is incorrect. You cannot use CloudFront to pull data directly from an EBS volume.

INCORRECT: "Configure CloudFront to require users to access the files using a signed URL, and configure the S3 bucket as a website endpoint" is incorrect. You cannot use CloudFront and an OAI when your S3 bucket is configured as a website endpoint.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

SET 2: PRACTICE QUESTIONS ONLY

For training purposes, go directly to [Set 2: Practice Questions, Answers & Explanations](#)

QUESTION 1

A group of business analysts perform read-only SQL queries on an Amazon RDS database. The queries have become quite numerous and the database has experienced some performance degradation. The queries must be run against the latest data. A Solutions Architect must solve the performance problems with minimal changes to the existing web application.

What should the Solutions Architect recommend?

1. Export the data to Amazon S3 and instruct the business analysts to run their queries using Amazon Athena.
2. Load the data into an Amazon Redshift cluster and instruct the business analysts to run their queries against the cluster.
3. Load the data into Amazon ElastiCache and instruct the business analysts to run their queries against the ElastiCache endpoint.
4. Create a read replica of the primary database and instruct the business analysts to direct queries to the replica.

QUESTION 2

A company is planning to upload a large quantity of sensitive data to Amazon S3. The company's security department require that the data is encrypted before it is uploaded.

Which option meets these requirements?

1. Use server-side encryption with customer-provided encryption keys.
2. Use client-side encryption with a master key stored in AWS KMS.
3. Use client-side encryption with Amazon S3 managed encryption keys.
4. Use server-side encryption with keys stored in KMS.

QUESTION 3

An application running on Amazon ECS processes data and then writes objects to an Amazon S3 bucket. The application requires permissions to make the S3 API calls.

How can a Solutions Architect ensure the application has the required permissions?

1. Update the S3 policy in IAM to allow read/write access from Amazon ECS, and then relaunch the container.
2. Create a set of Access Keys with read/write permissions to the bucket and update the task credential ID.
3. Create an IAM role that has read/write permissions to the bucket and update the task definition to specify the role as the taskRoleArn.
4. Attach an IAM policy with read/write permissions to the bucket to an IAM group and add the container instances to the group.

QUESTION 4

An application upgrade caused some issues with stability. The application owner enabled logging and has generated a 5 GB log file in an Amazon S3 bucket. The log file must be securely shared with the application vendor to troubleshoot the issues.

What is the MOST secure way to share the log file?

1. Create access keys using an administrative account and share the access key ID and secret access key with the vendor.
2. Enable default encryption for the bucket and public access. Provide the S3 URL of the file to the vendor.
3. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.
4. Generate a presigned URL and ask the vendor to download the log file before the URL expires.

QUESTION 5

A company has a file share on a Microsoft Windows Server in an on-premises data center. The server uses a local network attached storage (NAS) device to store several terabytes of files. The management team require a reduction in the data center footprint and to minimize storage costs by moving on-premises storage to AWS.

What should a Solutions Architect do to meet these requirements

1. Create an Amazon EFS volume and use an IPSec VPN.
2. Configure an AWS Storage Gateway file gateway.
3. Create an Amazon S3 bucket and an S3 gateway endpoint.
4. Configure an AWS Storage Gateway as a volume gateway.

QUESTION 6

A company uses a Microsoft Windows file share for storing documents and media files. Users access the share using Microsoft Windows clients and are authenticated using the company's Active Directory. The chief information officer wants to move the data to AWS as they are approaching capacity limits. The existing user authentication and access management system should be used.

How can a Solutions Architect meet these requirements?

1. Move the documents and media files to an Amazon FSx for Windows File Server file system.
2. Move the documents and media files to an Amazon Elastic File System and use POSIX permissions.
3. Move the documents and media files to an Amazon FSx for Lustre file system.
4. Move the documents and media files to an Amazon Simple Storage Service bucket and apply bucket ACLs.

QUESTION 7

A company runs an internal application for logging customer support information. The application runs on Amazon EC2 instances in an Auto Scaling group. The ASG scales up to 10 instances during business hours and scales down to 2 instances overnight. Staff have complained of poor performance at the beginning of the business day.

How should a Solutions Architect configure the Auto Scaling group to resolve the performance issues whilst minimizing costs?

1. Implement a step scaling action with a lower CPU threshold and decrease the cooldown period.
2. Implement a scheduled action that sets the minimum and maximum capacity to 10 before business hours begin.
3. Implement a target tracking action with a lower CPU threshold, and decrease the cooldown period.
4. Implement a scheduled action that sets the desired capacity to 10 before business hours begin.

QUESTION 8

A company requires a solution for replicating data to AWS for disaster recovery. Currently, the company uses scripts to copy data from various sources to a Microsoft Windows file server in the on-premises data center. The company also requires that a small amount of recent files are accessible to administrators with low latency.

What should a Solutions Architect recommend to meet these requirements?

1. Update the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises file server.
2. Update the script to copy data to an Amazon EBS volume instead of the on-premises file server.
3. Update the script to copy data to an Amazon EFS volume instead of the on-premises file server.
4. Update the script to copy data to an Amazon S3 Glacier archive instead of the on-premises file server.

QUESTION 9

A company runs an application in an Amazon VPC that requires access to an Amazon Elastic Container Service (Amazon ECS) cluster that hosts an application in another VPC. The company's security team requires that all traffic must not traverse the internet.

Which solution meets this requirement?

1. Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the VPC that hosts the ECS cluster.
2. Configure a gateway endpoint for Amazon ECS. Update the route table to include an entry pointing to the ECS cluster.
3. Configure an Amazon Route 53 private hosted zone for each VPC. Use private records to resolve internal IP addresses in each VPC.
4. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC.

QUESTION 10

An application stores transactional data in an Amazon S3 bucket. The data is analyzed for the first week and then must remain immediately available for occasional analysis.

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

1. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.
2. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days.
3. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
4. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

QUESTION 11

A highly sensitive application runs on Amazon EC2 instances using EBS volumes. The application stores data temporarily on Amazon EBS volumes during processing before saving results to an Amazon RDS database. The company's security team mandate that the sensitive data must be encrypted at rest.

Which solution should a Solutions Architect recommend to meet this requirement?

1. Configure encryption for the Amazon EBS volumes and Amazon RDS database with AWS KMS keys.
2. Use AWS Certificate Manager to generate certificates that can be used to encrypt the connections between the EC2 instances and RDS.
3. Use Amazon Data Lifecycle Manager to encrypt all data as it is stored to the EBS volumes and RDS database.
4. Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes.

QUESTION 12

A company runs an eCommerce application that uses an Amazon Aurora database. The database performs well except for short periods when monthly sales reports are run. A Solutions Architect has reviewed metrics in Amazon CloudWatch and found that the Read Ops and CPUUtilization metrics are spiking during the periods when the sales reports are run.

What is the MOST cost-effective solution to solve this performance issue?

1. Create an Amazon Redshift data warehouse and run the reporting there.
2. Modify the Aurora database to use an instance class with more CPU.
3. Create an Aurora Replica and use the replica endpoint for reporting.
4. Enable storage Auto Scaling for the Amazon Aurora database.

QUESTION 13

A company runs an application on Amazon EC2 instances which requires access to sensitive data in an Amazon S3 bucket. All traffic between the EC2 instances and the S3 bucket must not traverse the internet and must use private IP addresses.

Additionally, the bucket must only allow access from services in the VPC.

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

1. Create a VPC endpoint for Amazon S3.
2. Apply a bucket policy to restrict access to the S3 endpoint.
3. Enable default encryption on the bucket.
4. Create a peering connection to the S3 bucket VPC.
5. Apply an IAM policy to a VPC peering connection.

QUESTION 14

A company wants to migrate a legacy web application from an on-premises data center to AWS. The web application consists of a web tier, an application tier, and a MySQL database. The company does not want to manage instances or clusters.

Which combination of services should a solutions architect include in the overall architecture? (Select TWO.)

1. Amazon DynamoDB

2. Amazon RDS for MySQL
3. Amazon EC2 Spot Instances
4. Amazon Kinesis Data Streams
5. AWS Fargate

QUESTION 15

A web application is being deployed on an Amazon ECS cluster using the Fargate launch type. The application is expected to receive a large volume of traffic initially. The company wishes to ensure that performance is good for the launch and that costs reduce as demand decreases.

What should a solutions architect recommend?

1. Use Amazon EC2 Auto Scaling to scale out on a schedule and back in once the load decreases.
2. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
3. Use Amazon ECS Service Auto Scaling with target tracking policies to scale when an Amazon CloudWatch alarm is breached.
4. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when an Amazon CloudWatch alarm is breached.

QUESTION 16

A company runs several NFS file servers in an on-premises data center. The NFS servers must run periodic backups to Amazon S3 using automatic synchronization for small volumes of data.

Which solution meets these requirements and is MOST cost-effective?

1. Set up AWS Glue to extract the data from the NFS shares and load it into Amazon S3.
2. Set up an AWS DataSync agent on the on-premises servers and sync the data to Amazon S3.
3. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3.
4. Set up an AWS Direct Connect connection between the on-premises data center and AWS and copy the data to Amazon S3.

QUESTION 17

An organization plans to deploy a higher performance computing (HPC) workload on AWS using Linux. The HPC workload will use many Amazon EC2 instances and will generate a large quantity of small output files that must be stored in persistent storage for future use.

A Solutions Architect must design a solution that will enable the EC2 instances to access data using native file system interfaces and to store output files in cost-effective long-term storage.

Which combination of AWS services meets these requirements?

1. Amazon FSx for Lustre with Amazon S3.
2. Amazon FSx for Windows File Server with Amazon S3.
3. Amazon EBS volumes with Amazon S3 Glacier.
4. AWS DataSync with Amazon S3 Intelligent tiering.

QUESTION 18

An application has been deployed on Amazon EC2 instances behind an Application Load Balancer (ALB). A Solutions Architect must improve the security posture of the application and minimize the impact of a DDoS attack on resources.

Which of the following solutions is MOST effective?

1. Configure an AWS WAF ACL with rate-based rules. Enable the WAF ACL on the Application Load Balancer.
2. Create a custom AWS Lambda function that monitors for suspicious traffic and modifies a network ACL when a potential DDoS attack is identified.
3. Enable VPC Flow Logs and store them in Amazon S3. Use Amazon Athena to parse the logs and identify and block potential DDoS attacks.
4. Enable access logs on the Application Load Balancer and configure Amazon CloudWatch to monitor the access logs and trigger a Lambda function when potential attacks are identified. Configure the Lambda function to modify the ALBs security group and block the attack.

QUESTION 19

An automotive company plans to implement IoT sensors in manufacturing equipment that will send data to AWS in real time. The solution must receive events in an ordered manner from each asset and ensure that the data is saved for future processing.

Which solution would be MOST efficient?

1. 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.
2. 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.
3. 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.
4. 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.

QUESTION 20

An IoT sensor is being rolled out to thousands of a company's existing customers. The sensors will stream high volumes of data each second to a central location. A solution must be designed to ingest and store the data for analytics. The solution must provide near-real time performance and millisecond responsiveness.

Which solution should a Solutions Architect recommend?

1. Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon RedShift.
2. Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon DynamoDB.
3. Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon DynamoDB.
4. Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon RedShift.

QUESTION 21

A company runs a number of core enterprise applications in an on-premises data center. The data center is connected to an Amazon VPC using AWS Direct Connect. The company will be creating additional AWS accounts and these accounts will also need to be quickly, and cost-effectively connected to the on-premises data center in order to access the core applications.

What deployment changes should a Solutions Architect implement to meet these requirements with the LEAST operational overhead?

1. Create a Direct Connect connection in each new account. Route the network traffic to the on-premises servers.
2. Configure VPC endpoints in the Direct Connect VPC for all required services. Route the network traffic to the on-premises servers.
3. Create a VPN connection between each new account and the Direct Connect VPC. Route the network traffic to the on-premises servers.
4. Configure AWS Transit Gateway between the accounts. Assign Direct Connect to the transit gateway and route network traffic to the on-premises servers.

QUESTION 22

A solutions architect has been tasked with designing a highly resilient hybrid cloud architecture connecting an on-premises data center and AWS. The network should include AWS Direct Connect (DX).

Which DX configuration offers the HIGHEST resiliency?

1. Configure a DX connection with an encrypted VPN on top of it.
2. Configure multiple public VIFs on top of a DX connection.
3. Configure multiple private VIFs on top of a DX connection.
4. Configure DX connections at multiple DX locations.

QUESTION 23

A website is running on Amazon EC2 instances and access is restricted to a limited set of IP ranges. A solutions architect is planning to migrate static content from the website to an Amazon S3 bucket configured as an origin for an Amazon CloudFront distribution. Access to the static content must be restricted to the same set of IP addresses.

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

1. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
2. Create an origin access identity (OAI) and associate it with the distribution. Generate presigned URLs that limit access to the OAI.
3. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the Amazon S3 bucket.
4. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.
5. Attach the existing security group that contains the IP restrictions to the Amazon CloudFront distribution.

QUESTION 24

A company is storing a large quantity of small files in an Amazon S3 bucket. An application running on an Amazon EC2 instance needs permissions to access and process the files in the S3 bucket.

Which action will MOST securely grant the EC2 instance access to the S3 bucket?

1. Create a bucket ACL on the S3 bucket and configure the EC2 instance ID as a grantee.
2. Create an IAM role with least privilege permissions and attach it to the EC2 instance profile.
3. Create an IAM user for the application with specific permissions to the S3 bucket.
4. Generate access keys and store the credentials on the EC2 instance for use in making API calls.

QUESTION 25

A company requires a solution to allow customers to customize images that are stored in an online catalog. The image customization parameters will be sent in requests to Amazon API Gateway. The customized image will then be generated on-demand and can be accessed online.

The solutions architect requires a highly available solution. Which solution will be MOST cost-effective?

1. Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances
2. Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin
3. Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances
4. Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin

QUESTION 26

A solutions architect is finalizing the architecture for a distributed database that will run across multiple Amazon EC2 instances. Data will be replicated across all instances so the loss of an instance will not cause loss of data. The database requires block storage with low latency and throughput that supports up to several million transactions per second per server.

Which storage solution should the solutions architect use?

1. Amazon EBS
2. Amazon EC2 instance store
3. Amazon EFS
4. Amazon S3

QUESTION 27

A website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website's DNS records are hosted in Amazon Route 53 with the domain name pointing to the ALB. A solution is required for displaying a static error page if the website becomes unavailable.

Which configuration should a solutions architect use to meet these requirements with the LEAST operational overhead?

1. Create a Route 53 alias record for an Amazon CloudFront distribution and specify the ALB as the origin. Create custom error pages for the distribution
2. Create a Route 53 active-passive failover configuration. Create a static website using an Amazon S3 bucket that hosts a static error page. Configure the static website as the passive record for failover
3. Create a Route 53 weighted routing policy. Create a static website using an Amazon S3 bucket that hosts a static error page. Configure the record for the S3 static website with a weighting of zero. When an issue occurs increase the weighting
4. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB

QUESTION 28

A company is deploying a new web application that will run on Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. The application requires a shared storage solution that offers strong consistency as the content will be regularly updated.

Which solution requires the LEAST amount of effort?

1. Create an Amazon S3 bucket to store the web content and use Amazon CloudFront to deliver the content
2. Create an Amazon Elastic File System (Amazon EFS) file system and mount it on the individual Amazon EC2 instances
3. Create a shared Amazon Block Store (Amazon EBS) volume and mount it on the individual Amazon EC2 instances
4. Create a volume gateway using AWS Storage Gateway to host the data and mount it to the Auto Scaling group

QUESTION 29

A web application has recently been launched on AWS. The architecture includes two tier with a web layer and a database layer. It has been identified that the web server layer may be vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

1. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF
2. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF
3. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF
4. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard

QUESTION 30

A multi-tier application runs with eight front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer. A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

1. Create an Auto Scaling group that uses four instances across each of two Regions
2. Modify the Auto Scaling group to use four instances across each of two Availability Zones
3. Create an Auto Scaling template that can be used to quickly create more instances in another Region
4. Create an Auto Scaling group that uses four instances across each of two subnets

QUESTION 31

A company's web application is using multiple Amazon EC2 Linux instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure.

What should a solutions architect do to meet these requirements?

1. Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance

2. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance
3. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance
4. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-A)

QUESTION 32

A website runs on a Microsoft Windows server in an on-premises data center. The web server is being migrated to Amazon EC2 Windows instances in multiple Availability Zones on AWS. The web server currently uses data stored in an on-premises network-attached storage (NAS) device.

Which replacement to the NAS file share is MOST resilient and durable?

1. Migrate the file share to Amazon EBS
2. Migrate the file share to AWS Storage Gateway
3. Migrate the file share to Amazon FSx for Windows File Server
4. Migrate the file share to Amazon Elastic File System (Amazon EFS)

QUESTION 33

A company is planning a migration for a high performance computing (HPC) application and associated data from an on-premises data center to the AWS Cloud. The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO.)

1. Amazon S3 for cold data storage
2. Amazon EFS for cold data storage
3. Amazon S3 for high-performance parallel storage
4. Amazon FSx for Lustre for high-performance parallel storage
5. Amazon FSx for Windows for high-performance parallel storage

QUESTION 34

A web application that allows users to upload and share documents is running on a single Amazon EC2 instance with an Amazon EBS volume. To increase availability the architecture has been updated to use an Auto Scaling group of several instances across Availability Zones behind an Application Load Balancer. After the change users can only see a subset of the documents.

What is the BEST method for a solutions architect to modify the solution so users can see all documents?

1. Run a script to synchronize the data between Amazon EBS volumes
2. Use Sticky Sessions with the ALB to ensure users are directed to the same EC2 instance in a session
3. Copy the data from all EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS
4. Configure the Application Load Balancer to send the request to all servers. Return each document from the correct server

QUESTION 35

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 midmorning

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

1. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens
2. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period
3. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period
4. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens

QUESTION 36

An application uses Amazon EC2 instances and an Amazon RDS MySQL database. The database is not currently encrypted. A solutions architect needs to apply encryption to the database for all new and existing data.

How should this be accomplished?

1. Create an Amazon ElastiCache cluster and encrypt data using the cache nodes
2. Enable encryption for the database using the API. Take a full snapshot of the database. Delete old snapshots
3. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot
4. 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

QUESTION 37

A company have 500 TB of data in an on-premises file share that needs to be moved to Amazon S3 Glacier. The migration must not saturate the company's low-bandwidth internet connection and the migration must be completed within a few weeks.

What is the MOST cost-effective solution?

1. Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier
2. Order 7 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint
3. Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth
4. Order 7 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier

QUESTION 38

A company has refactored a legacy application to run as two microservices using Amazon ECS. The application processes data in two parts and the second part of the process takes longer than the first.

How can a solutions architect integrate the microservices and allow them to scale independently?

1. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2
2. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic
3. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose
4. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue

QUESTION 39

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.)

1. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0
2. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0
3. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier
4. 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
5. 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

QUESTION 40

A solutions architect has created a new AWS account and must secure AWS account root user access.

Which combination of actions will accomplish this? (Select TWO.)

1. Ensure the root user uses a strong password
2. Enable multi-factor authentication to the root user
3. Store root user access keys in an encrypted Amazon S3 bucket
4. Add the root user to a group containing administrative permissions
5. Delete the root user account

QUESTION 41

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 solutions architect address this issue?

1. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
2. Use service control policies to disable IAM activity across all accounts in the organizational unit
3. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
4. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

QUESTION 42

A solutions architect is optimizing a website for real-time streaming and on-demand videos. The website's users are located around the world and the solutions architect needs to optimize the performance for both the real-time and on-demand streaming.

Which service should the solutions architect choose?

1. Amazon CloudFront
2. AWS Global Accelerator
3. Amazon Route 53
4. Amazon S3 Transfer Acceleration

QUESTION 43

Objects uploaded to Amazon S3 are initially accessed frequently for a period of 30 days. Then, objects are infrequently accessed for up to 90 days. After that, the objects are no longer needed.

How should lifecycle management be configured?

1. Transition to STANDARD_IA after 30 days. After 90 days transition to GLACIER
2. Transition to STANDARD_IA after 30 days. After 90 days transition to ONEZONE_IA
3. Transition to ONEZONE_IA after 30 days. After 90 days expire the objects
4. Transition to REDUCED_REDUNDANCY after 30 days. After 90 days expire the objects

QUESTION 44

A company has acquired another business and needs to migrate their 50TB of data into AWS within 1 month. They also require a secure, reliable and private connection to the AWS cloud.

How are these requirements best accomplished?

1. Provision an AWS Direct Connect connection and migrate the data over the link
2. Migrate data using AWS Snowball. Provision an AWS VPN initially and order a Direct Connect link
3. Launch a Virtual Private Gateway (VPG) and migrate the data over the AWS VPN
4. Provision an AWS VPN CloudHub connection and migrate the data over redundant links

QUESTION 45

An application on Amazon Elastic Container Service (ECS) performs data processing in two parts. The second part takes much

longer to complete. How can an Architect decouple the data processing from the backend application component?

1. Process both parts using the same ECS task. Create an Amazon Kinesis Firehose stream
2. Process each part using a separate ECS task. Create an Amazon SNS topic and send a notification when the processing completes
3. Create an Amazon DynamoDB table and save the output of the first part to the table
4. Process each part using a separate ECS task. Create an Amazon SQS queue

QUESTION 46

An application is running on Amazon EC2 behind an Elastic Load Balancer (ELB). Content is being published using Amazon CloudFront and you need to restrict the ability for users to circumvent CloudFront and access the content directly through the ELB.

How can you configure this solution?

1. Create an Origin Access Identity (OAI) and associate it with the distribution
2. Use signed URLs or signed cookies to limit access to the content
3. Use a Network ACL to restrict access to the ELB
4. Create a VPC Security Group for the ELB and use AWS Lambda to automatically update the CloudFront internal service IP addresses when they change

QUESTION 47

A company has divested a single business unit and needs to move the AWS account owned by the business unit to another AWS Organization. How can this be achieved?

1. Create a new account in the destination AWS Organization and migrate resources
2. Create a new account in the destination AWS Organization and share the original resources using AWS Resource Access Manager
3. Migrate the account using AWS CloudFormation
4. Migrate the account using the AWS Organizations console

QUESTION 48

An Amazon RDS PostgreSQL database is configured as Multi-AZ. A solutions architect needs to scale read performance and the solution must be configured for high availability. What is the most cost-effective solution?

1. Create a read replica as a Multi-AZ DB instance
2. Deploy a read replica in a different AZ to the master DB instance
3. Deploy a read replica using Amazon ElastiCache
4. Deploy a read replica in the same AZ as the master DB instance

QUESTION 49

A High Performance Computing (HPC) application will be migrated to AWS. The application requires low network latency and high throughput between nodes and will be deployed in a single AZ.

How should the application be deployed for best inter-node performance?

1. In a partition placement group
2. In a cluster placement group
3. In a spread placement group
4. Behind a Network Load Balancer (NLB)

QUESTION 50

A web application is deployed in multiple regions behind an ELB Application Load Balancer. You need deterministic routing to the closest region and automatic failover. Traffic should traverse the AWS global network for consistent performance.

How can this be achieved?

1. Configure AWS Global Accelerator and configure the ALBs as targets
2. Place an EC2 Proxy in front of the ALB and configure automatic failover

3. Create a Route 53 Alias record for each ALB and configure a latency-based routing policy
4. Use a CloudFront distribution with multiple custom origins in each region and configure for high availability

QUESTION 51

A company's Amazon EC2 instances were terminated or stopped, resulting in a loss of important data that was stored on attached EC2 instance stores. They want to avoid this happening in the future and need a solution that can scale as data volumes increase with the LEAST amount of management and configuration.

Which storage is most appropriate?

1. Amazon EFS
2. Amazon S3
3. Amazon EBS
4. Amazon RDS

QUESTION 52

An application launched on Amazon EC2 instances needs to publish personally identifiable information (PII) about customers using Amazon SNS. The application is launched in private subnets within an Amazon VPC.

Which is the MOST secure way to allow the application to access service endpoints in the same region?

1. Use an Internet Gateway
2. Use AWS PrivateLink
3. Use a proxy instance
4. Use a NAT gateway

QUESTION 53

A Solutions Architect is designing a web application that runs on Amazon EC2 instances behind an Elastic Load Balancer. All data in transit must be encrypted.

Which solution options meet the encryption requirement? (Select TWO.)

1. Use a Network Load Balancer (NLB) with a TCP listener, then terminate SSL on EC2 instances
2. Use an Application Load Balancer (ALB) with an HTTPS listener, then install SSL certificates on the ALB and EC2 instances
3. Use an Application Load Balancer (ALB) in passthrough mode, then terminate SSL on EC2 instances
4. Use a Network Load Balancer (NLB) with an HTTPS listener, then install SSL certificates on the NLB and EC2 instances
5. Use an Application Load Balancer (ALB) with a TCP listener, then terminate SSL on EC2 instances

QUESTION 54

An application running video-editing software is using significant memory on an Amazon EC2 instance. How can a user track memory usage on the Amazon EC2 instance?

1. Install the CloudWatch agent on the EC2 instance to push memory usage to an Amazon CloudWatch custom metric
2. Use an instance type that supports memory usage reporting to a metric by default
3. Call Amazon CloudWatch to retrieve the memory usage metric data that exists for the EC2 instance
4. Assign an IAM role to the EC2 instance with an IAM policy granting access to the desired metric

QUESTION 55

An organization is migrating data to the AWS cloud. An on-premises application uses Network File System shares and must access the data without code changes. The data is critical and is accessed frequently.

Which storage solution should a Solutions Architect recommend to maximize availability and durability?

1. Amazon Elastic Block Store
2. Amazon Simple Storage Service
3. AWS Storage Gateway – File Gateway
4. Amazon Elastic File System

QUESTION 56

A Solutions Architect needs to design a solution that will allow Website Developers to deploy static web content without managing server infrastructure. All web content must be accessed over HTTPS with a custom domain name. The solution should be scalable as the company continues to grow.

Which of the following will provide the MOST cost-effective solution?

1. Amazon S3 with a static website
2. Amazon CloudFront with an Amazon S3 bucket origin
3. AWS Lambda function with Amazon API Gateway
4. Amazon EC2 instance with Amazon EBS

QUESTION 57

A Solutions Architect must design a storage solution for incoming billing reports in CSV format. The data will be analyzed infrequently and discarded after 30 days.

Which combination of services will be MOST cost-effective in meeting these requirements?

1. Write the files to an S3 bucket and use Amazon Athena to query the data
2. Import the logs to an Amazon Redshift cluster
3. Use AWS Data Pipeline to import the logs into a DynamoDB table
4. Import the logs into an RDS MySQL instance

QUESTION 58

A Solutions Architect must design a solution that encrypts data in Amazon S3. Corporate policy mandates encryption keys be generated and managed on premises. Which solution should the Architect use to meet the security requirements?

1. SSE-C: Server-side encryption with customer-provided encryption keys
2. SSE-S3: Server-side encryption with Amazon-managed master key
3. SSE-KMS: Server-side encryption with AWS KMS managed keys
4. AWS CloudHSM

QUESTION 59

A Solutions Architect must select the most appropriate database service for two use cases. A team of data scientists perform complex queries on a data warehouse that take several hours to complete. Another team of scientists need to run fast, repeat queries and update dashboards for customer support staff.

Which solution delivers these requirements MOST cost-effectively?

1. RedShift for both use cases
2. RDS for both use cases
3. RedShift for the analytics use case and ElastiCache in front of RedShift for the customer support dashboard
4. RedShift for the analytics use case and RDS for the customer support dashboard

QUESTION 60

A DynamoDB database you manage is randomly experiencing heavy read requests that are causing latency. What is the simplest way to alleviate the performance issues?

1. Create DynamoDB read replicas
2. Enable EC2 Auto Scaling for DynamoDB
3. Create an ElastiCache cluster in front of DynamoDB
4. Enable DynamoDB DAX

QUESTION 61

A large media site has multiple applications running on Amazon ECS. A Solutions Architect needs to use content metadata to route traffic to specific services.

What is the MOST efficient method to fulfil this requirement?

1. Use an AWS Classic Load Balancer with a host-based routing rule to route traffic to the correct service
2. Use the AWS CLI to update an Amazon Route 53 hosted zone to route traffic as services get updated
3. Use an AWS Application Load Balancer with a path-based routing rule to route traffic to the correct service
4. Use Amazon CloudFront to manage and route traffic to the correct service

QUESTION 62

You have created a file system using Amazon Elastic File System (EFS) which will hold home directories for users. What else needs to be done to enable users to save files to the EFS file system?

1. Create a separate EFS file system for each user and grant read-write-execute permissions on the root directory to the respective user. Then mount the file system to the users' home directory
2. Modify permissions on the root directory to grant read-write-execute permissions to the users. Then create a subdirectory and mount it to the users' home directory
3. Instruct the users to create a subdirectory on the file system and mount the subdirectory to their home directory
4. Create a subdirectory for each user and grant read-write-execute permissions to the users. Then mount the subdirectory to the users' home directory

QUESTION 63

An AWS workload in a VPC is running a legacy database on an Amazon EC2 instance. Data is stored on a 2000GB Amazon EBS (gp2) volume. At peak load times, logs show excessive wait time.

What should be implemented to improve database performance using persistent storage?

1. Change the EC2 instance type to one with burstable performance
2. Change the EC2 instance type to one with EC2 instance store volumes
3. Migrate the data on the Amazon EBS volume to an SSD-backed volume
4. Migrate the data on the EBS volume to provisioned IOPS SSD (io1)

QUESTION 64

A data-processing application runs on an i3.large EC2 instance with a single 100 GB EBS gp2 volume. The application stores temporary data in a small database (less than 30 GB) located on the EBS root volume. The application is struggling to process the data fast enough, and a Solutions Architect has determined that the I/O speed of the temporary database is the bottleneck.

What is the MOST cost-efficient way to improve the database response times?

1. Put the temporary database on a new 50-GB EBS io1 volume with a 3000 IOPS allocation
2. Move the temporary database onto instance storage
3. Put the temporary database on a new 50-GB EBS gp2 volume
4. Enable EBS optimization on the instance and keep the temporary files on the existing volume

QUESTION 65

An application is hosted on the U.S west coast. Users there have no problems, but users on the east coast are experiencing performance issues. The users have reported slow response times with the search bar autocomplete and display of account listings.

How can you improve the performance for users on the east coast?

1. Host the static content in an Amazon S3 bucket and distribute it using CloudFront
2. Setup cross-region replication and use Route 53 geolocation routing
3. Create a DynamoDB Read Replica in the U.S east region
4. Create an ElastiCache database in the U.S east region

SET 2: PRACTICE QUESTIONS AND ANSWERS

QUESTION 1

A group of business analysts perform read-only SQL queries on an Amazon RDS database. The queries have become quite numerous and the database has experienced some performance degradation. The queries must be run against the latest data. A Solutions Architect must solve the performance problems with minimal changes to the existing web application.

What should the Solutions Architect recommend?

1. Export the data to Amazon S3 and instruct the business analysts to run their queries using Amazon Athena.
2. Load the data into an Amazon Redshift cluster and instruct the business analysts to run their queries against the cluster.
3. Load the data into Amazon ElastiCache and instruct the business analysts to run their queries against the ElastiCache endpoint.
4. Create a read replica of the primary database and instruct the business analysts to direct queries to the replica.

Answer: 4

Explanation:

The performance issues can be easily resolved by offloading the SQL queries the business analysts are performing to a read replica. This ensures that data that is being queried is up to date and the existing web application does not require any modifications to take place.

CORRECT: "Create a read replica of the primary database and instruct the business analysts to direct queries to the replica" is the correct answer.

INCORRECT: "Export the data to Amazon S3 and instruct the business analysts to run their queries using Amazon Athena" is incorrect. The data must be the latest data and this method would therefore require constant exporting of the data.

INCORRECT: "Load the data into an Amazon Redshift cluster and instruct the business analysts to run their queries against the cluster" is incorrect. This is another solution that requires exporting the loading the data which means over time it will become out of date.

INCORRECT: "Load the data into Amazon ElastiCache and instruct the business analysts to run their queries against the ElastiCache endpoint" is incorrect. It will be much easier to create a read replica. ElastiCache requires updates to the application code so should be avoided in this example.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 2

A company is planning to upload a large quantity of sensitive data to Amazon S3. The company's security department require that the data is encrypted before it is uploaded.

Which option meets these requirements?

1. Use server-side encryption with customer-provided encryption keys.
2. Use client-side encryption with a master key stored in AWS KMS.
3. Use client-side encryption with Amazon S3 managed encryption keys.
4. Use server-side encryption with keys stored in KMS.

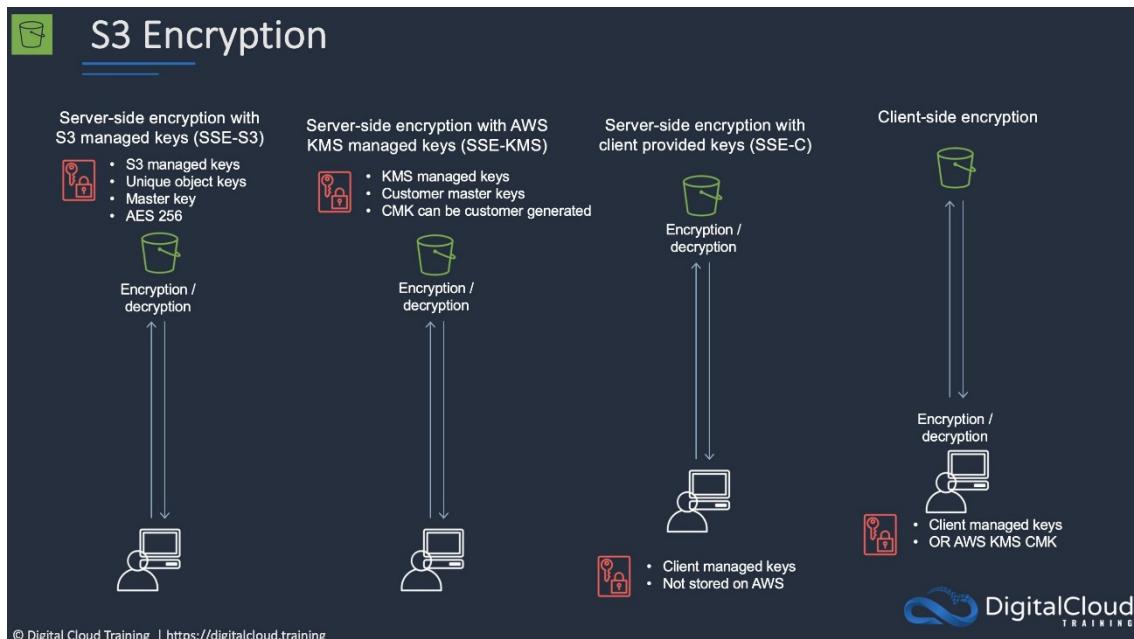
Answer: 2

Explanation:

The requirement is that the objects must be encrypted before they are uploaded. The only option presented that meets this requirement is to use client-side encryption. You then have two options for the keys you use to perform the encryption:

- Use a customer master key (CMK) stored in AWS Key Management Service (AWS KMS).
- Use a master key that you store within your application.

In this case the correct answer is to use an AWS KMS key. Note that you cannot use client-side encryption with keys managed by Amazon S3.



CORRECT: "Use client-side encryption with a master key stored in AWS KMS" is the correct answer.

INCORRECT: "Use client-side encryption with Amazon S3 managed encryption keys" is incorrect. You cannot use S3 managed keys with client-side encryption.

INCORRECT: "Use server-side encryption with customer-provided encryption keys" is incorrect. With this option the encryption takes place after uploading to S3.

INCORRECT: "Use server-side encryption with keys stored in KMS" is incorrect. With this option the encryption takes place after uploading to S3.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingClientSideEncryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 3

An application running on Amazon ECS processes data and then writes objects to an Amazon S3 bucket. The application requires permissions to make the S3 API calls.

How can a Solutions Architect ensure the application has the required permissions?

1. Update the S3 policy in IAM to allow read/write access from Amazon ECS, and then relaunch the container.
2. Create a set of Access Keys with read/write permissions to the bucket and update the task credential ID.
3. Create an IAM role that has read/write permissions to the bucket and update the task definition to specify the role as the taskRoleArn.
4. Attach an IAM policy with read/write permissions to the bucket to an IAM group and add the container instances to the group.

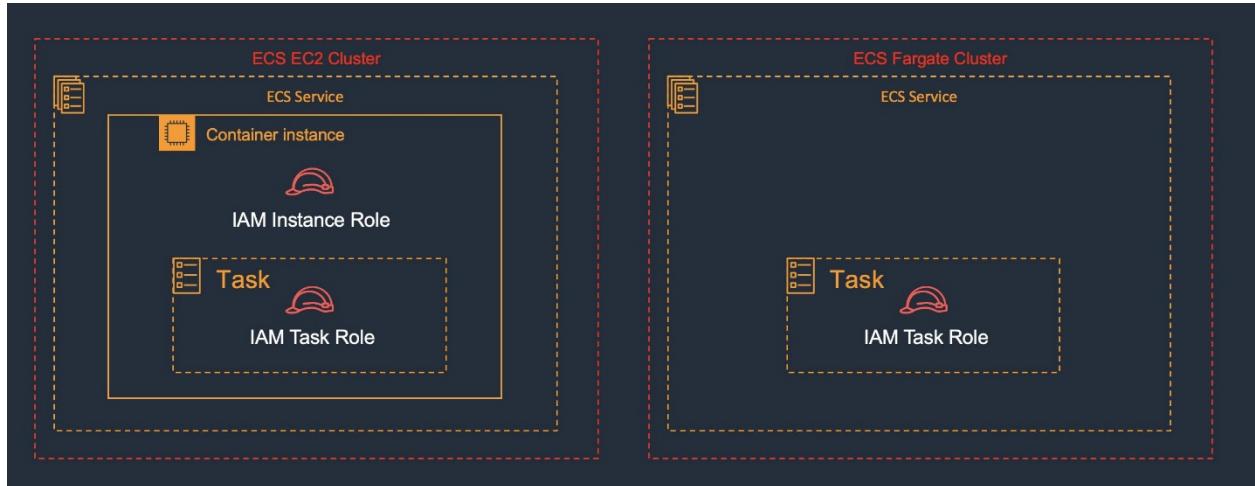
Answer: 3

Explanation:

With IAM roles for Amazon ECS tasks, you can specify an IAM role that can be used by the containers in a task. Applications must sign their AWS API requests with AWS credentials, and this feature provides a strategy for managing credentials for your applications to use, similar to the way that Amazon EC2 instance profiles provide credentials to EC2 instances.

You define the IAM role to use in your task definitions, or you can use a taskRoleArn override when running a task manually with the RunTask API operation.

Note that there are instances roles and task roles that you can assign in ECS when using the EC2 launch type. The task role is better when you need to assign permissions for just that specific task:



Correct: "Create an IAM role that has read/write permissions to the bucket and update the task definition to specify the role as the taskRoleArn" is the correct answer.

Incorrect: "Update the S3 policy in IAM to allow read/write access from Amazon ECS, and then relaunch the container" is incorrect. Policies must be assigned to tasks using IAM Roles and this is not mentioned here.

Incorrect: "Create a set of Access Keys with read/write permissions to the bucket and update the task credential ID" is incorrect. You cannot update the task credential ID with access keys and roles should be used instead.

Incorrect: "Attach an IAM policy with read/write permissions to the bucket to an IAM group and add the container instances to the group" is incorrect. You cannot add container instances to an IAM group.

References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

QUESTION 4

An application upgrade caused some issues with stability. The application owner enabled logging and has generated a 5 GB log file in an Amazon S3 bucket. The log file must be securely shared with the application vendor to troubleshoot the issues.

What is the MOST secure way to share the log file?

1. Create access keys using an administrative account and share the access key ID and secret access key with the vendor.
2. Enable default encryption for the bucket and public access. Provide the S3 URL of the file to the vendor.
3. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.
4. Generate a presigned URL and ask the vendor to download the log file before the URL expires.

Answer: 4

Explanation:

A presigned URL gives you access to the object identified in the URL. When you create a presigned URL, you must provide your security credentials and then specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The presigned URLs are valid only for the specified duration. That is, you must start the action before the expiration date and time.

This is the most secure way to provide the vendor with time-limited access to the log file in the S3 bucket.

CORRECT: "Generate a presigned URL and ask the vendor to download the log file before the URL expires" is the correct answer.

INCORRECT: "Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication" is incorrect. This is less secure as you have to create an account to access AWS and then ensure you lock down the account appropriately.

INCORRECT: "Create access keys using an administrative account and share the access key ID and secret access key with the vendor" is incorrect. This is extremely insecure as the access keys will provide administrative permissions to AWS and should never be shared.

INCORRECT: "Enable default encryption for the bucket and public access. Provide the S3 URL of the file to the vendor" is incorrect. Encryption does not assist here as the bucket would be public and anyone could access it.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ShareObjectPreSignedURL.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 5

A company has a file share on a Microsoft Windows Server in an on-premises data center. The server uses a local network attached storage (NAS) device to store several terabytes of files. The management team require a reduction in the data center footprint and to minimize storage costs by moving on-premises storage to AWS.

What should a Solutions Architect do to meet these requirements

1. Create an Amazon EFS volume and use an IPsec VPN.
2. Configure an AWS Storage Gateway file gateway.
3. Create an Amazon S3 bucket and an S3 gateway endpoint.
4. Configure an AWS Storage Gateway as a volume gateway.

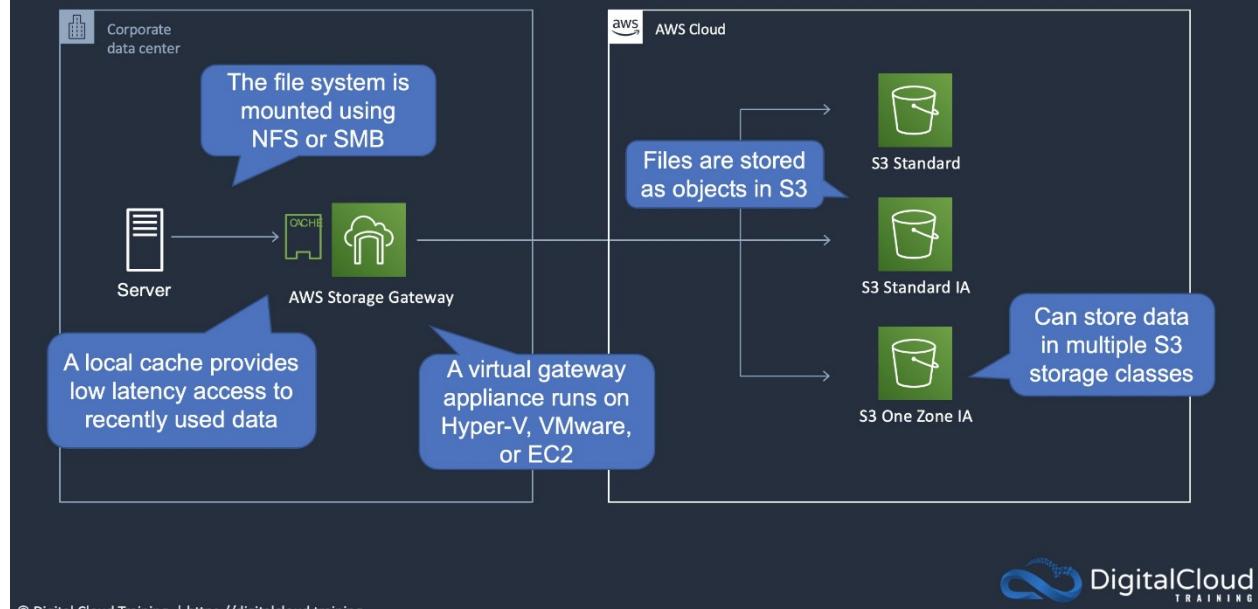
Answer: 2

Explanation:

An AWS Storage Gateway File Gateway provides your applications a file interface to seamlessly store files as objects in Amazon S3, and access them using industry standard file protocols. This removes the files from the on-premises NAS device and provides a method of directly mounting the file share for on-premises servers and clients.



AWS Storage Gateway – File Gateway



© DigitalCloud Training | <https://digitalcloud.training>



CORRECT: "Configure an AWS Storage Gateway file gateway" is the correct answer.

INCORRECT: "Configure an AWS Storage Gateway as a volume gateway" is incorrect. A volume gateway uses block-based protocols. In this case we are replacing a NAS device which uses file-level protocols so the best option is a file gateway.

INCORRECT: "Create an Amazon EFS volume and use an IPSec VPN" is incorrect. EFS can be mounted over a VPN but it would have more latency than using a storage gateway.

INCORRECT: "Create an Amazon S3 bucket and an S3 gateway endpoint" is incorrect. S3 is an object-level storage system so is not suitable for this use case. A gateway endpoint is a method of accessing S3 using private addresses from your VPC, not from your data center.

References:

<https://aws.amazon.com/storagegateway/faqs/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

QUESTION 6

A company uses a Microsoft Windows file share for storing documents and media files. Users access the share using Microsoft Windows clients and are authenticated using the company's Active Directory. The chief information officer wants to move the data to AWS as they are approaching capacity limits. The existing user authentication and access management system should be used.

How can a Solutions Architect meet these requirements?

1. Move the documents and media files to an Amazon FSx for Windows File Server file system.
2. Move the documents and media files to an Amazon Elastic File System and use POSIX permissions.
3. Move the documents and media files to an Amazon FSx for Lustre file system.
4. Move the documents and media files to an Amazon Simple Storage Service bucket and apply bucket ACLs.

Answer: 1

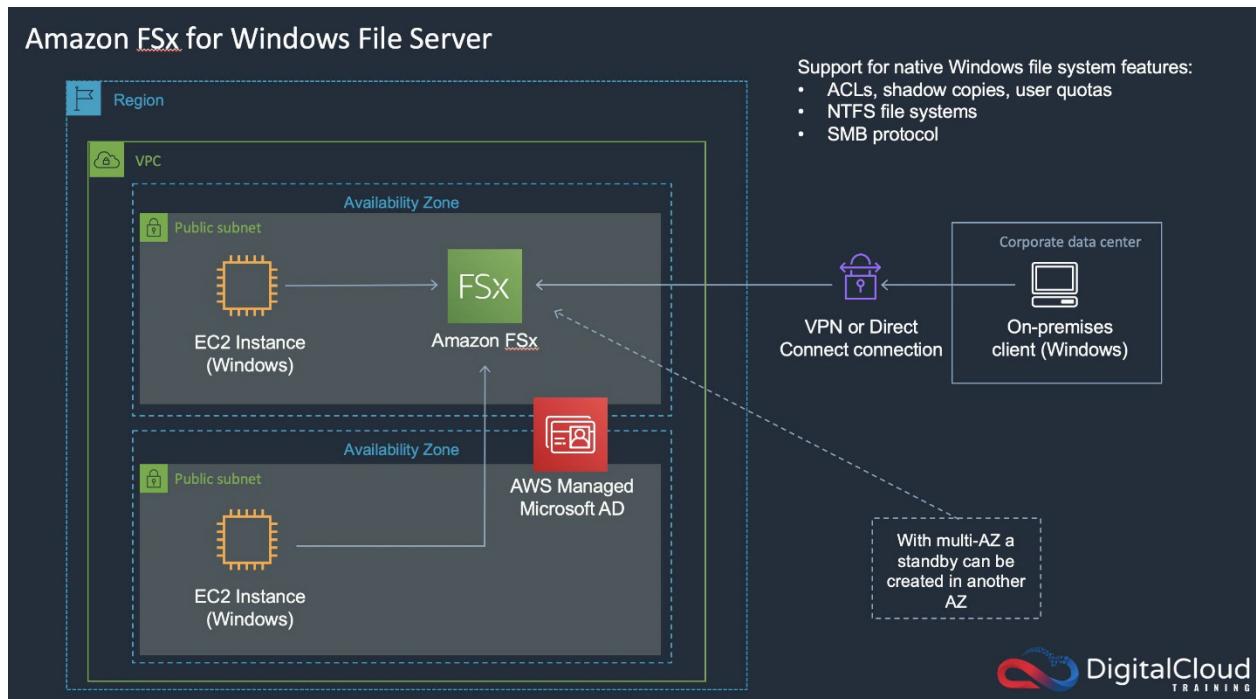
Explanation:

Amazon FSx for Windows File Server makes it easy for you to launch and scale reliable, performant, and secure shared file storage for your applications and end users. With Amazon FSx, you can launch highly durable and available file systems that can

span multiple availability zones (AZs) and can be accessed from up to thousands of compute instances using the industry-standard Server Message Block (SMB) protocol.

It provides a rich set of administrative and security features, and integrates with Microsoft Active Directory (AD). To serve a wide spectrum of workloads, Amazon FSx provides high levels of file system throughput and IOPS and consistent sub-millisecond latencies.

You can also mount FSx file systems from on-premises using a VPN or Direct Connect connection. This topology is depicted in the image below:



CORRECT: "Move the documents and media files to an Amazon FSx for Windows File Server file system" is the correct answer.

INCORRECT: "Move the documents and media files to an Amazon FSx for Lustre file system" is incorrect. FSx for Lustre is not suitable for migrating a Microsoft Windows File Server implementation.

INCORRECT: "Move the documents and media files to an Amazon Elastic File System and use POSIX permissions" is incorrect. EFS can be used from on-premises over a VPN or DX connection but POSIX permissions are very different to Microsoft permissions and mean a different authentication and access management solution is required.

INCORRECT: "Move the documents and media files to an Amazon Simple Storage Service bucket and apply bucket ACLs" is incorrect. S3 with bucket ACLs would be changing to an object-based storage system and a completely different authentication and access management solution.

References:

<https://aws.amazon.com/fsx/windows/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 7

A company runs an internal application for logging customer support information. The application runs on Amazon EC2 instances in an Auto Scaling group. The ASG scales up to 10 instances during business hours and scales down to 2 instances overnight. Staff have complained of poor performance at the beginning of the business day.

How should a Solutions Architect configure the Auto Scaling group to resolve the performance issues whilst minimizing costs?

1. Implement a step scaling action with a lower CPU threshold and decrease the cooldown period.

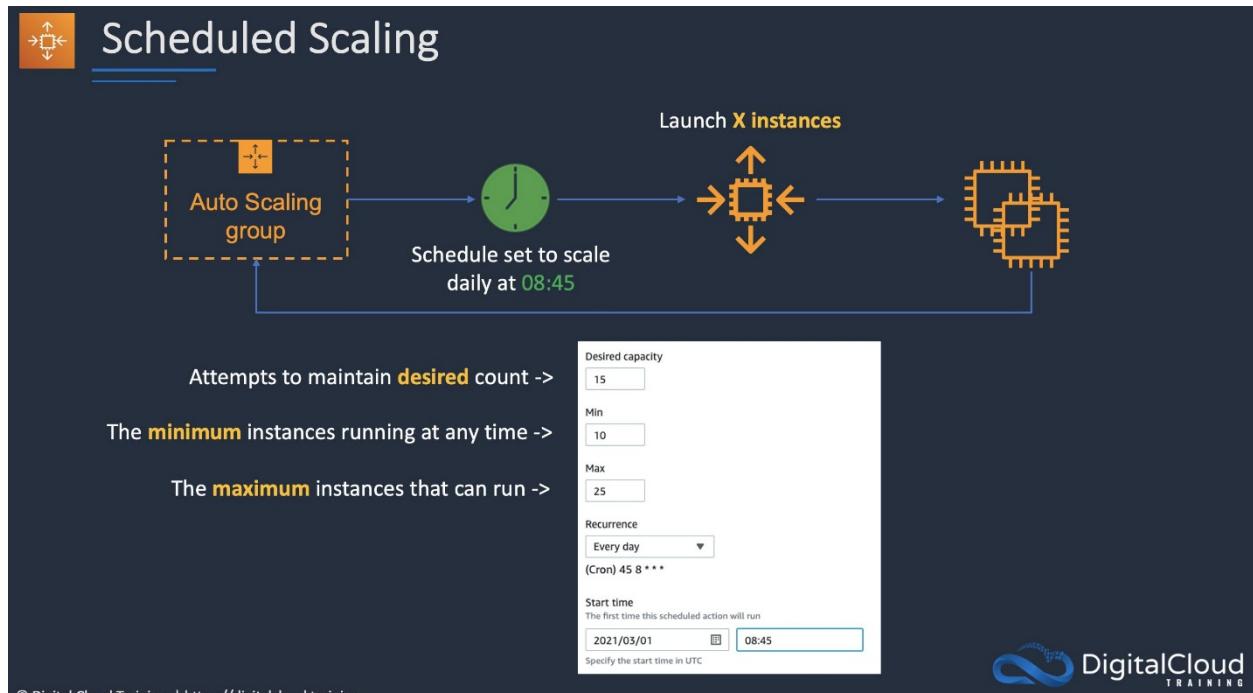
2. Implement a scheduled action that sets the minimum and maximum capacity to 10 before business hours begin.
3. Implement a target tracking action with a lower CPU threshold, and decrease the cooldown period.
4. Implement a scheduled action that sets the desired capacity to 10 before business hours begin.

Answer: 4

Explanation:

Scheduled scaling allows you to set your own scaling schedule. In this example it means the Solutions Architect can configure the scaling action to take place shortly before business hours begin and that will ensure adequate capacity exists from the very beginning of the business day.

In this example below the scheduled scaling policy is configured to scale at 08:45am daily with a desired count of 15. This will result in 15 instances being available shortly after.



© Digital Cloud Training | <https://digitalcloud.training>

CORRECT: "Implement a scheduled action that sets the desired capacity to 10 before business hours begin" is the correct answer.

INCORRECT: "Implement a scheduled action that sets the minimum and maximum capacity to 10 before business hours begin" is incorrect. The minimum and maximums define how many instances CAN run; the desired capacity sets how many you WANT to be running.

INCORRECT: "Implement a step scaling action with a lower CPU threshold and decrease the cooldown period" is incorrect. A cooldown period will result in faster scaling and a lower CPU threshold will cause scaling to happen at a lower loads. However, there is still a lag time before the instances are available to service users and this could result in too many instances running for the rest of the day.

INCORRECT: "Implement a target tracking action with a lower CPU threshold, and decrease the cooldown period" is incorrect. As above, this may achieve faster scaling at lower loads but is also going to be higher cost and applications may still not be ready for the beginning of the business day.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 8

A company requires a solution for replicating data to AWS for disaster recovery. Currently, the company uses scripts to copy data from various sources to a Microsoft Windows file server in the on-premises data center. The company also requires that a small amount of recent files are accessible to administrators with low latency.

What should a Solutions Architect recommend to meet these requirements?

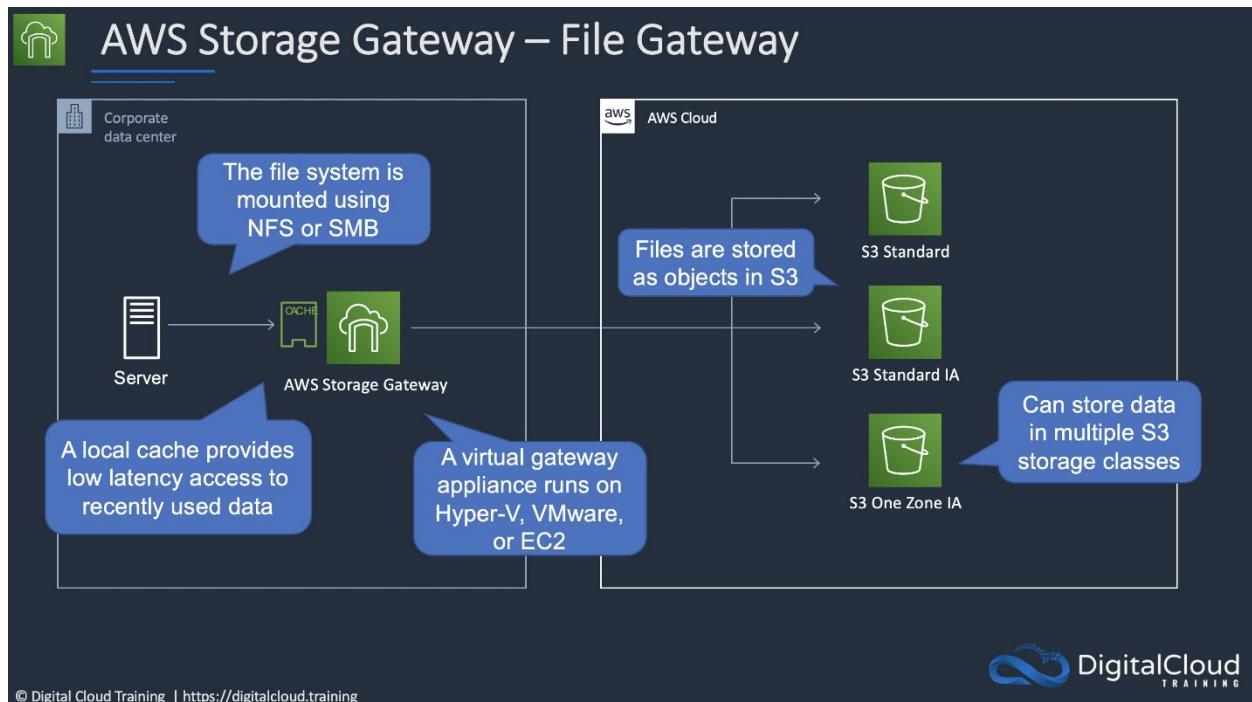
1. Update the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises file server.
2. Update the script to copy data to an Amazon EBS volume instead of the on-premises file server.
3. Update the script to copy data to an Amazon EFS volume instead of the on-premises file server.
4. Update the script to copy data to an Amazon S3 Glacier archive instead of the on-premises file server.

Answer: 1

Explanation:

The best solution here is to use an AWS Storage Gateway File Gateway virtual appliance in the on-premises data center. This can be accessed the same protocols as the existing Microsoft Windows File Server (SMB/CIFS). Therefore, the script simply needs to be updated to point to the gateway.

The file gateway will then store data on Amazon S3 and has a local cache for data that can be accessed at low latency. The file gateway provides an excellent method of enabling file protocol access to low cost S3 object storage.



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Update the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises file server" is the correct answer.

INCORRECT: "Update the script to copy data to an Amazon EBS volume instead of the on-premises file server" is incorrect. This would also need an attached EC2 instance running Windows to be able to mount using the same protocols and would not offer any local low-latency access.

INCORRECT: "Update the script to copy data to an Amazon EFS volume instead of the on-premises file server" is incorrect. This solution would not provide a local cache.

INCORRECT: "Update the script to copy data to an Amazon S3 Glacier archive instead of the on-premises file server" is incorrect. This would not provide any immediate access with low-latency.

References:

<https://aws.amazon.com/storagegateway/file/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 9

A company runs an application in an Amazon VPC that requires access to an Amazon Elastic Container Service (Amazon ECS) cluster that hosts an application in another VPC. The company's security team requires that all traffic must not traverse the internet.

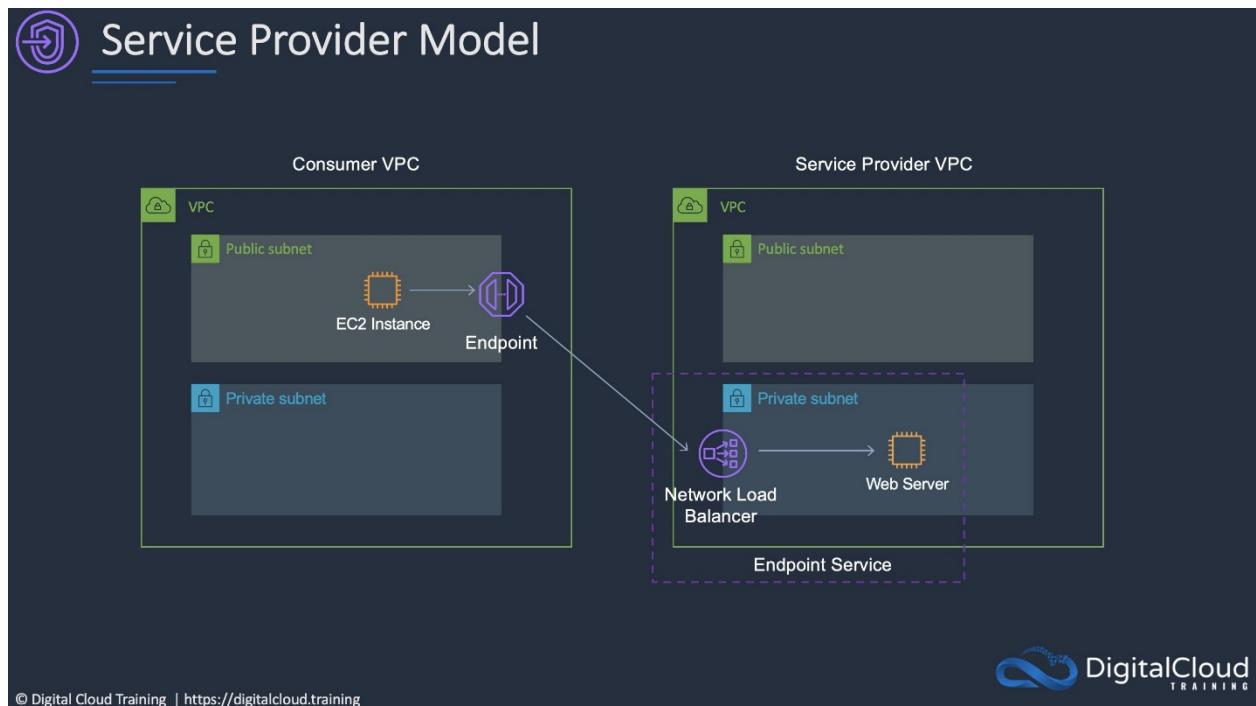
Which solution meets this requirement?

1. Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the VPC that hosts the ECS cluster.
2. Configure a gateway endpoint for Amazon ECS. Update the route table to include an entry pointing to the ECS cluster.
3. Configure an Amazon Route 53 private hosted zone for each VPC. Use private records to resolve internal IP addresses in each VPC.
4. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC.

Answer: 4

Explanation:

The correct solution is to use AWS PrivateLink in a service provider model. In this configuration a network load balancer will be implemented in the service provider VPC (the one with the ECS cluster in this example), and a PrivateLink endpoint will be created in the consumer VPC (the one with the company's application).



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC" is the correct answer.

INCORRECT: "Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the VPC that hosts the ECS cluster" is incorrect. The endpoint should be in the consumer VPC, not the service provider VPC (see the diagram above).

INCORRECT: "Configure a gateway endpoint for Amazon ECS. Update the route table to include an entry pointing to the ECS cluster" is incorrect. You cannot use a gateway endpoint to connect to a private service. Gateway endpoints are only for S3 and DynamoDB.

INCORRECT: "Configure an Amazon Route 53 private hosted zone for each VPC. Use private records to resolve internal IP addresses in each VPC" is incorrect. This does not provide a mechanism for resolving each other's addresses and there's no method of internal communication using private IPs such as VPC peering.

References:

<https://aws.amazon.com/privatelink/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 10

An application stores transactional data in an Amazon S3 bucket. The data is analyzed for the first week and then must remain immediately available for occasional analysis.

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

1. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.
2. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days.
3. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
4. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Answer: 3

Explanation:

The transition should be to Standard-IA rather than One Zone-IA. Though One Zone-IA would be cheaper, it also offers lower availability and the question states the objects "must remain immediately available". Therefore the availability is a consideration.

Though there is no minimum duration when storing data in S3 Standard, you cannot transition to Standard IA within 30 days. This can be seen when trying to create a lifecycle rule:

Transition current versions of objects between storage classes

Storage class transitions	Days after object creation	
Standard-IA	7	Remove transition

A minimum of 30 days is required before transitioning to Standard-IA.

Add transition

Therefore, the best solution is to transition after 30 days.

CORRECT: "Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days" is the correct answer.

INCORRECT: "Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days" is incorrect as explained above.

INCORRECT: "Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days" is incorrect as explained above.

INCORRECT: "Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days" is incorrect as explained above.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 11

A highly sensitive application runs on Amazon EC2 instances using EBS volumes. The application stores data temporarily on Amazon EBS volumes during processing before saving results to an Amazon RDS database. The company's security team mandate that the sensitive data must be encrypted at rest.

Which solution should a Solutions Architect recommend to meet this requirement?

1. Configure encryption for the Amazon EBS volumes and Amazon RDS database with AWS KMS keys.
2. Use AWS Certificate Manager to generate certificates that can be used to encrypt the connections between the EC2 instances and RDS.
3. Use Amazon Data Lifecycle Manager to encrypt all data as it is stored to the EBS volumes and RDS database.
4. Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes.

Answer: 1

Explanation:

As the data is stored both in the EBS volumes (temporarily) and the RDS database, both the EBS and RDS volumes must be encrypted at rest. This can be achieved by enabling encryption at creation time of the volume and AWS KMS keys can be used to encrypt the data. This solution meets all requirements.

CORRECT: "Configure encryption for the Amazon EBS volumes and Amazon RDS database with AWS KMS keys" is the correct answer.

INCORRECT: "Use AWS Certificate Manager to generate certificates that can be used to encrypt the connections between the EC2 instances and RDS" is incorrect. This would encrypt the data in-transit but not at-rest.

INCORRECT: "Use Amazon Data Lifecycle Manager to encrypt all data as it is stored to the EBS volumes and RDS database" is incorrect. DLM is used for automating the process of taking and managing snapshots for EBS volumes.

INCORRECT: "Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes" is incorrect. You cannot configure SSL/TLS encryption using KMS CMKs or use SSL/TLS to encrypt data at rest.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 12

A company runs an eCommerce application that uses an Amazon Aurora database. The database performs well except for short periods when monthly sales reports are run. A Solutions Architect has reviewed metrics in Amazon CloudWatch and found that the Read Ops and CPUUtilization metrics are spiking during the periods when the sales reports are run.

What is the MOST cost-effective solution to solve this performance issue?

1. Create an Amazon Redshift data warehouse and run the reporting there.
2. Modify the Aurora database to use an instance class with more CPU.
3. Create an Aurora Replica and use the replica endpoint for reporting.
4. Enable storage Auto Scaling for the Amazon Aurora database.

Answer: 3

Explanation:

The simplest and most cost-effective option is to use an Aurora Replica. The replica can serve read operations which will mean

the reporting application can run reports on the replica endpoint without causing any performance impact on the production database.

CORRECT: "Create an Aurora Replica and use the replica endpoint for reporting" is the correct answer.

INCORRECT: "Enable storage Auto Scaling for the Amazon Aurora database" is incorrect. Aurora storage automatically scales based on volumes, there is no storage auto scaling feature for Aurora.

INCORRECT: "Create an Amazon Redshift data warehouse and run the reporting there" is incorrect. This would be less cost-effective and require more work in copying the data to the data warehouse.

INCORRECT: "Modify the Aurora database to use an instance class with more CPU" is incorrect. This may not resolve the storage performance issues and could be more expensive depending on instances sizes.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.StorageReliability.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>

QUESTION 13

A company runs an application on Amazon EC2 instances which requires access to sensitive data in an Amazon S3 bucket. All traffic between the EC2 instances and the S3 bucket must not traverse the internet and must use private IP addresses. Additionally, the bucket must only allow access from services in the VPC.

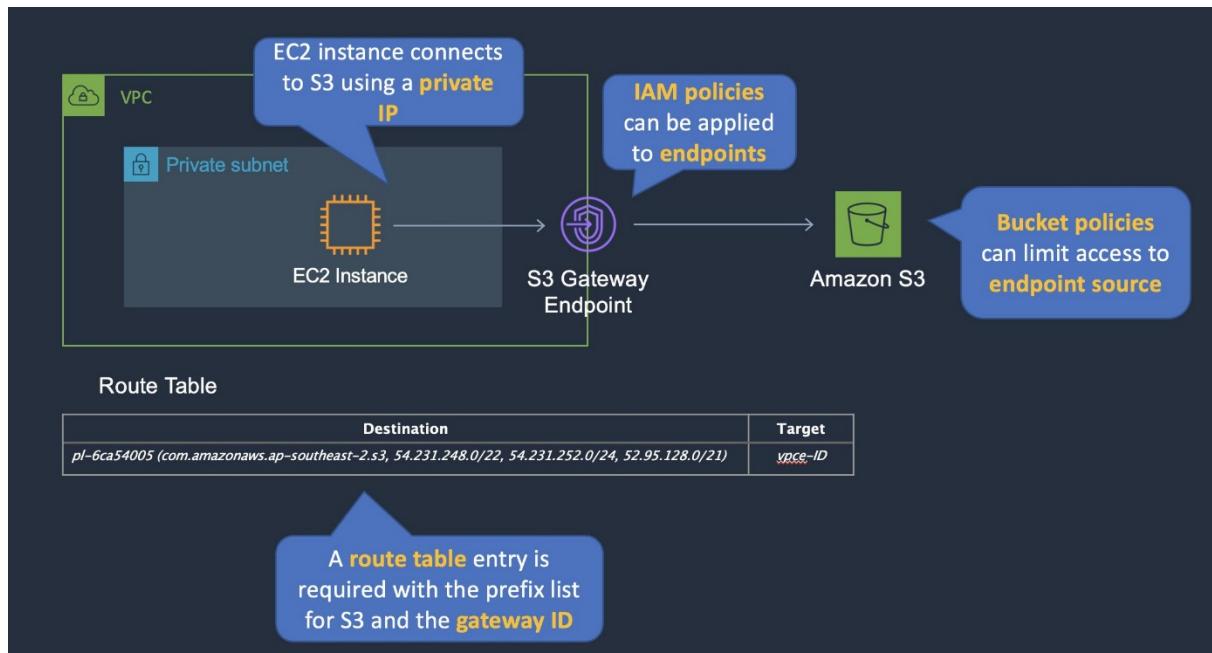
Which combination of actions should a Solutions Architect take to meet these requirements? (Select TWO.)

1. Create a VPC endpoint for Amazon S3.
2. Apply a bucket policy to restrict access to the S3 endpoint.
3. Enable default encryption on the bucket.
4. Create a peering connection to the S3 bucket VPC.
5. Apply an IAM policy to a VPC peering connection.

Answer: 1,2

Explanation:

Private access to public services such as Amazon S3 can be achieved by creating a VPC endpoint in the VPC. For S3 this would be a gateway endpoint. The bucket policy can then be configured to restrict access to the S3 endpoint only which will ensure that only services originating from the VPC will be granted access.



CORRECT: "Create a VPC endpoint for Amazon S3" is a correct answer.

CORRECT: "Apply a bucket policy to restrict access to the S3 endpoint" is also a correct answer.

INCORRECT: "Enable default encryption on the bucket" is incorrect. This will encrypt data at rest but does not restrict access.

INCORRECT: "Create a peering connection to the S3 bucket VPC" is incorrect. You cannot create a peering connection to S3 as it is a public service and does not run in a VPC.

INCORRECT: "Apply an IAM policy to a VPC peering connection" is incorrect. You cannot apply an IAM policy to a peering connection.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 14

A company wants to migrate a legacy web application from an on-premises data center to AWS. The web application consists of a web tier, an application tier, and a MySQL database. The company does not want to manage instances or clusters.

Which combination of services should a solutions architect include in the overall architecture? (Select TWO.)

1. Amazon DynamoDB
2. Amazon RDS for MySQL
3. Amazon EC2 Spot Instances
4. Amazon Kinesis Data Streams
5. AWS Fargate

Answer: 2,5

Explanation:

Amazon RDS is a managed service and you do not need to manage the instances. This is an ideal backend for the application and you can run a MySQL database on RDS without any refactoring. For the application components these can run on Docker containers with AWS Fargate. Fargate is a serverless service for running containers on AWS.

CORRECT: "AWS Fargate" is a correct answer.

CORRECT: "Amazon RDS for MySQL" is also a correct answer.

INCORRECT: "Amazon DynamoDB" is incorrect. This is a NoSQL database and would be incompatible with the relational MySQL DB.

INCORRECT: "Amazon EC2 Spot Instances" is incorrect. This would require managing instances.

INCORRECT: "Amazon Kinesis Data Streams" is incorrect. This is a service for streaming data.

References:

<https://aws.amazon.com/rds/>

<https://aws.amazon.com/fargate/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 15

A web application is being deployed on an Amazon ECS cluster using the Fargate launch type. The application is expected to receive a large volume of traffic initially. The company wishes to ensure that performance is good for the launch and that costs reduce as demand decreases

What should a solutions architect recommend?

1. Use Amazon EC2 Auto Scaling to scale out on a schedule and back in once the load decreases.
2. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
3. Use Amazon ECS Service Auto Scaling with target tracking policies to scale when an Amazon CloudWatch alarm is breached.
4. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when an Amazon CloudWatch alarm is breached.

Answer: 3

Explanation:

Amazon ECS uses the AWS Application Auto Scaling service to scales tasks. This is configured through Amazon ECS using Amazon ECS Service Auto Scaling.

A Target Tracking Scaling policy increases or decreases the number of tasks that your service runs based on a target value for a specific metric. For example, in the image below the tasks will be scaled when the average CPU breaches 80% (as reported by CloudWatch):

Scaling policy type Target tracking Step scaling

Policy name*

ECS service metric*

Configure an ALB for the service in order to enable target tracking on ALB metrics

Target value*

Scale-out cooldown period seconds between scaling actions

Scale-in cooldown period seconds between scaling actions

Disable scale-in

CORRECT: "Use Amazon ECS Service Auto Scaling with target tracking policies to scale when an Amazon CloudWatch alarm is breached" is the correct answer.

INCORRECT: "Use Amazon EC2 Auto Scaling with simple scaling policies to scale when an Amazon CloudWatch alarm is breached" is incorrect

INCORRECT: "Use Amazon EC2 Auto Scaling to scale out on a schedule and back in once the load decreases" is incorrect

INCORRECT: "Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm" is incorrect

References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

QUESTION 16

A company runs several NFS file servers in an on-premises data center. The NFS servers must run periodic backups to Amazon S3 using automatic synchronization for small volumes of data.

Which solution meets these requirements and is MOST cost-effective?

1. Set up AWS Glue to extract the data from the NFS shares and load it into Amazon S3.
2. Set up an AWS DataSync agent on the on-premises servers and sync the data to Amazon S3.
3. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3.
4. Set up an AWS Direct Connect connection between the on-premises data center and AWS and copy the data to Amazon S3.

Answer: 2

Explanation:

AWS DataSync is an online data transfer service that simplifies, automates, and accelerates copying large amounts of data between on-premises systems and AWS Storage services, as well as between AWS Storage services. DataSync can copy data between Network File System (NFS) shares, or Server Message Block (SMB) shares, self-managed object storage, [AWS Snowcone](#), [Amazon Simple Storage Service \(Amazon S3\)](#) buckets, [Amazon Elastic File System \(Amazon EFS\)](#) file systems,

and [Amazon FSx for Windows File Server](#) file systems.

This is the most cost-effective solution from the answer options available.

CORRECT: "Set up an AWS DataSync agent on the on-premises servers and sync the data to Amazon S3" is the correct answer.

INCORRECT: "Set up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3" is incorrect. This solution does not provide the scheduled synchronization features of AWS DataSync and is more expensive.

INCORRECT: "Set up AWS Glue to extract the data from the NFS shares and load it into Amazon S3" is incorrect. AWS Glue is an ETL service and cannot be used for copying data to Amazon S3 from NFS shares.

INCORRECT: "Set up an AWS Direct Connect connection between the on-premises data center and AWS and copy the data to Amazon S3" is incorrect. An AWS Direct Connect connection is an expensive option and no solution is provided for automatic synchronization.

References:

<https://aws.amazon.com/datasync/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-database-migration-service/>

QUESTION 17

An organization plans to deploy a higher performance computing (HPC) workload on AWS using Linux. The HPC workload will use many Amazon EC2 instances and will generate a large quantity of small output files that must be stored in persistent storage for future use.

A Solutions Architect must design a solution that will enable the EC2 instances to access data using native file system interfaces and to store output files in cost-effective long-term storage.

Which combination of AWS services meets these requirements?

1. Amazon FSx for Lustre with Amazon S3.
2. Amazon FSx for Windows File Server with Amazon S3.
3. Amazon EBS volumes with Amazon S3 Glacier.
4. AWS DataSync with Amazon S3 Intelligent tiering.

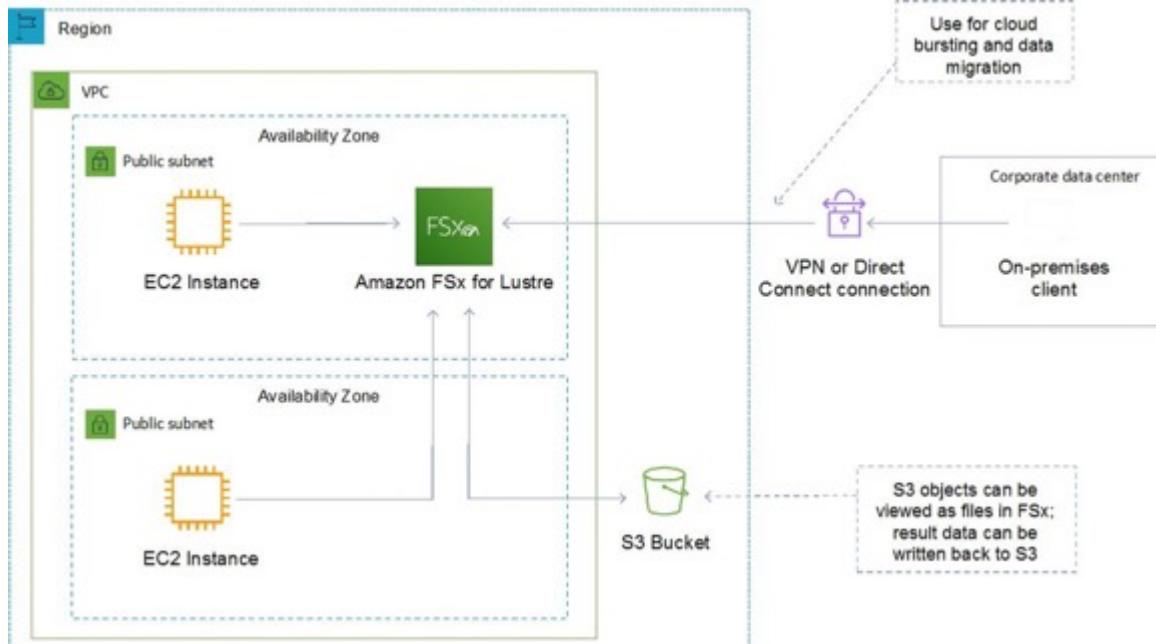
Answer: 1

Explanation:

Amazon FSx for Lustre is ideal for high performance computing (HPC) workloads running on Linux instances. FSx for Lustre provides a native file system interface and works as any file system does with your Linux operating system.

When linked to an Amazon S3 bucket, FSx for Lustre transparently presents objects as files, allowing you to run your workload without managing data transfer from S3.

This solution provides all requirements as it enables Linux workloads to use the native file system interfaces and to use S3 for long-term and cost-effective storage of output files.



CORRECT: "Amazon FSx for Lustre with Amazon S3" is the correct answer.

INCORRECT: "Amazon FSx for Windows File Server with Amazon S3" is incorrect. This service should be used with Windows instances and does not integrate with S3.

INCORRECT: "Amazon EBS volumes with Amazon S3 Glacier" is incorrect. EBS volumes do not provide the shared, high performance storage solution using file system interfaces.

INCORRECT: "AWS DataSync with Amazon S3 Intelligent tiering" is incorrect. AWS DataSync is used for migrating / synchronizing data.

References:

<https://aws.amazon.com/fsx/lustre/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 18

An application has been deployed on Amazon EC2 instances behind an Application Load Balancer (ALB). A Solutions Architect must improve the security posture of the application and minimize the impact of a DDoS attack on resources.

Which of the following solutions is MOST effective?

1. Configure an AWS WAF ACL with rate-based rules. Enable the WAF ACL on the Application Load Balancer.
2. Create a custom AWS Lambda function that monitors for suspicious traffic and modifies a network ACL when a potential DDoS attack is identified.
3. Enable VPC Flow Logs and store them in Amazon S3. Use Amazon Athena to parse the logs and identify and block potential DDoS attacks.
4. Enable access logs on the Application Load Balancer and configure Amazon CloudWatch to monitor the access logs and trigger a Lambda function when potential attacks are identified. Configure the Lambda function to modify the ALBs security group and block the attack.

Answer: 1

Explanation:

A rate-based rule tracks the rate of requests for each originating IP address, and triggers the rule action on IPs with rates that go over a limit. You set the limit as the number of requests per 5-minute time span.

You can use this type of rule to put a temporary block on requests from an IP address that's sending excessive requests. By default, AWS WAF aggregates requests based on the IP address from the web request origin, but you can configure the rule to use an IP address from an HTTP header, like X-Forwarded-For, instead.

CORRECT: "Configure an AWS WAF ACL with rate-based rules. Enable the WAF ACL on the Application Load Balancer" is the correct answer.

INCORRECT: "Create a custom AWS Lambda function that monitors for suspicious traffic and modifies a network ACL when a potential DDoS attack is identified" is incorrect. There's no description here of how Lambda is going to monitor for traffic.

INCORRECT: "Enable VPC Flow Logs and store them in Amazon S3. Use Amazon Athena to parse the logs and identify and block potential DDoS attacks" is incorrect. Amazon Athena is not able to block DDoS attacks, another service would be needed.

INCORRECT: "Enable access logs on the Application Load Balancer and configure Amazon CloudWatch to monitor the access logs and trigger a Lambda function when potential attacks are identified. Configure the Lambda function to modify the ALBs security group and block the attack" is incorrect. Access logs are exported to S3 but not to CloudWatch. Also, it would not be possible to block an attack from a specific IP using a security group (while still allowing any other source access) as they do not support deny rules.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-waf-and-shield/>

QUESTION 19

An automotive company plans to implement IoT sensors in manufacturing equipment that will send data to AWS in real time. The solution must receive events in an ordered manner from each asset and ensure that the data is saved for future processing. Which solution would be MOST efficient?

1. 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.
2. 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.
3. 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.
4. 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: 1

Explanation:

Amazon Kinesis Data Streams is the ideal service for receiving streaming data. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream. Therefore, a separate partition (rather than shard) should be used for each equipment asset.

Amazon Kinesis Firehose can be used to receive streaming data from Data Streams and then load the data into Amazon S3 for future processing.

CORRECT: "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" is the correct answer.

INCORRECT: "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" is incorrect. A partition should be used rather than a shard as explained above.

INCORRECT: "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" is incorrect. Amazon SQS cannot be used for real-time use cases.

INCORRECT: "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" is incorrect. Amazon SQS cannot be used for real-time use cases.

References:

<https://aws.amazon.com/kinesis/data-streams/faqs/>

<https://aws.amazon.com/kinesis/data-firehose/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>

QUESTION 20

An IoT sensor is being rolled out to thousands of a company's existing customers. The sensors will stream high volumes of data each second to a central location. A solution must be designed to ingest and store the data for analytics. The solution must provide near-real time performance and millisecond responsiveness.

Which solution should a Solutions Architect recommend?

1. Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon RedShift.
2. Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon DynamoDB.
3. Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon DynamoDB.
4. Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon RedShift.

Answer: 2

Explanation:

A Kinesis data stream is a set of shards. Each shard contains a sequence of data records. A **consumer** is an application that processes the data from a Kinesis data stream. You can map a Lambda function to a shared-throughput consumer (standard iterator), or to a dedicated-throughput consumer with enhanced fan-out.

Amazon DynamoDB is the best database for this use case as it supports near-real time performance and millisecond responsiveness.

CORRECT: "Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon DynamoDB" is the correct answer.

INCORRECT: "Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon RedShift" is incorrect. Amazon RedShift cannot provide millisecond responsiveness.

INCORRECT: "Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon RedShift" is incorrect. Amazon SQS does not provide near real-time performance and RedShift does not provide millisecond responsiveness.

INCORRECT: "Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon DynamoDB" is incorrect. Amazon SQS does not provide near real-time performance.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/with-kinesis.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>

QUESTION 21

A company runs a number of core enterprise applications in an on-premises data center. The data center is connected to an Amazon VPC using AWS Direct Connect. The company will be creating additional AWS accounts and these accounts will also need to be quickly, and cost-effectively connected to the on-premises data center in order to access the core applications.

What deployment changes should a Solutions Architect implement to meet these requirements with the LEAST operational overhead?

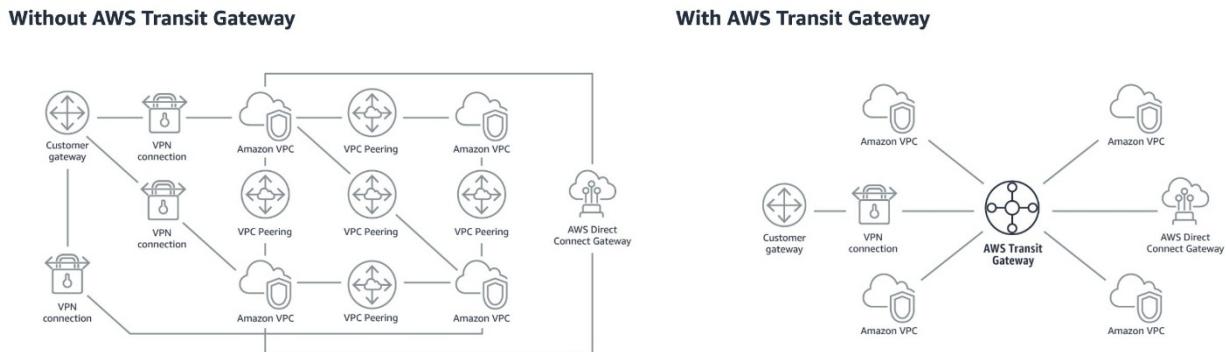
1. Create a Direct Connect connection in each new account. Route the network traffic to the on-premises servers.
2. Configure VPC endpoints in the Direct Connect VPC for all required services. Route the network traffic to the on-premises servers.
3. Create a VPN connection between each new account and the Direct Connect VPC. Route the network traffic to the on-premises servers.
4. Configure AWS Transit Gateway between the accounts. Assign Direct Connect to the transit gateway and route network traffic to the on-premises servers.

Answer: 4

Explanation:

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. With AWS Transit Gateway, you can quickly add Amazon VPCs, AWS accounts, VPN capacity, or AWS Direct Connect gateways to meet unexpected demand, without having to wrestle with complex connections or massive routing tables. This is the operationally least complex solution and is also cost-effective.

The image below depicts how transit gateway can assist with simplifying network deployments:



CORRECT: "Configure AWS Transit Gateway between the accounts. Assign Direct Connect to the transit gateway and route network traffic to the on-premises servers" is the correct answer.

INCORRECT: "Create a VPN connection between each new account and the Direct Connect VPC. Route the network traffic to the on-premises servers" is incorrect. You cannot connect VPCs using AWS managed VPNs and would need to configure a software VPN and then complex routing configurations. This is not the best solution.

INCORRECT: "Create a Direct Connect connection in each new account. Route the network traffic to the on-premises servers" is incorrect. This is an expensive solution as you would need to have multiple Direct Connect links.

INCORRECT: "Configure VPC endpoints in the Direct Connect VPC for all required services. Route the network traffic to the on-premises servers" is incorrect. You cannot create VPC endpoints for all services and this would be a complex solution for those you can.

References:

<https://aws.amazon.com/transit-gateway/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

QUESTION 22

A solutions architect has been tasked with designing a highly resilient hybrid cloud architecture connecting an on-premises data center and AWS. The network should include AWS Direct Connect (DX).

Which DX configuration offers the HIGHEST resiliency?

1. Configure a DX connection with an encrypted VPN on top of it.
2. Configure multiple public VIFs on top of a DX connection.
3. Configure multiple private VIFs on top of a DX connection.

- Configure DX connections at multiple DX locations.

Answer: 4

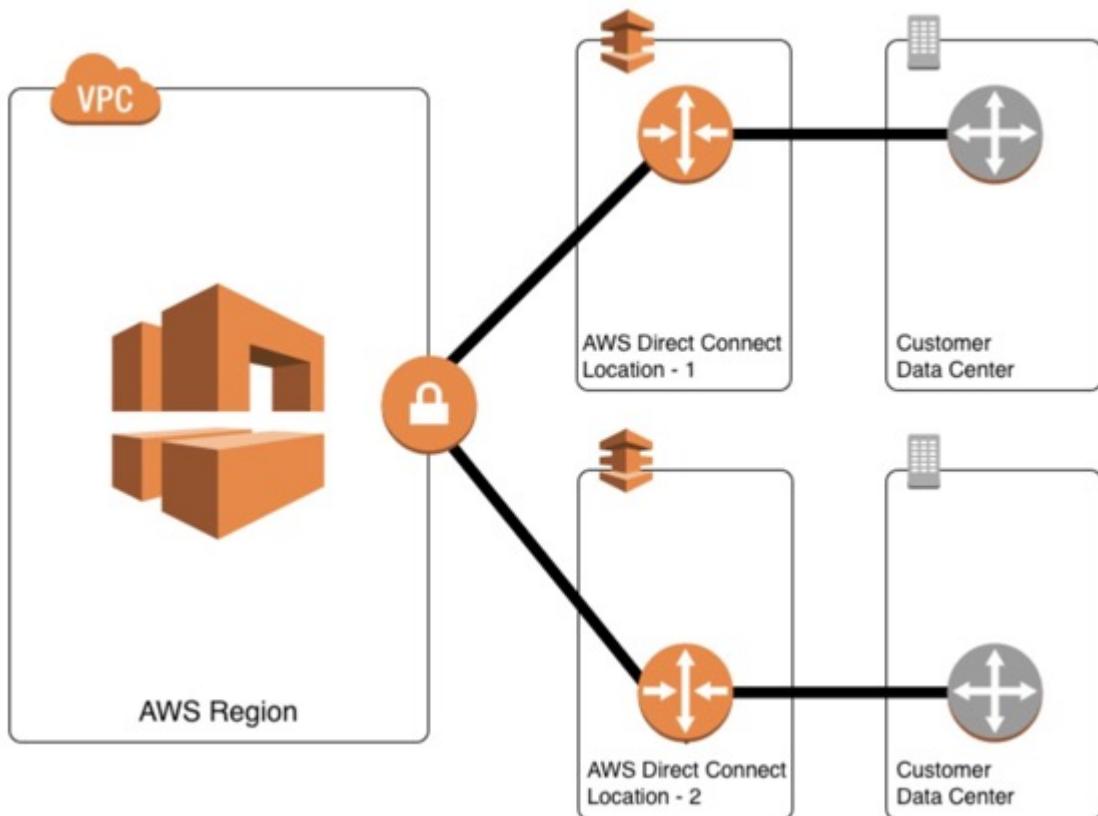
Explanation:

The most resilient solution is to configure DX connections at multiple DX locations. This ensures that any issues impacting a single DX location do not affect availability of the network connectivity to AWS.

Take note of the following AWS recommendations for resiliency:

AWS recommends connecting from multiple data centers for physical location redundancy. When designing remote connections, consider using redundant hardware and telecommunications providers. Additionally, it is a best practice to use dynamically routed, active/active connections for automatic load balancing and failover across redundant network connections. Provision sufficient network capacity to ensure that the failure of one network connection does not overwhelm and degrade redundant connections.

The diagram below is an example of an architecture that offers high resiliency:



CORRECT: "Configure DX connections at multiple DX locations" is the correct answer.

INCORRECT: "Configure a DX connection with an encrypted VPN on top of it" is incorrect. A VPN that is separate to the DX connection can be a good backup. But a VPN on top of the DX connection does not help. Also, encryption provides security but not resilience.

INCORRECT: "Configure multiple public VIFs on top of a DX connection" is incorrect. Virtual interfaces do not add resiliency as resiliency must be designed into the underlying connection.

INCORRECT: "Configure multiple private VIFs on top of a DX connection" is incorrect. Virtual interfaces do not add resiliency as resiliency must be designed into the underlying connection.

References:

<https://aws.amazon.com/directconnect/resiliency-recommendation/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

QUESTION 23

A website is running on Amazon EC2 instances and access is restricted to a limited set of IP ranges. A solutions architect is planning to migrate static content from the website to an Amazon S3 bucket configured as an origin for an Amazon CloudFront distribution. Access to the static content must be restricted to the same set of IP addresses.

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

1. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
2. Create an origin access identity (OAI) and associate it with the distribution. Generate presigned URLs that limit access to the OAI.
3. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the Amazon S3 bucket.
4. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.
5. Attach the existing security group that contains the IP restrictions to the Amazon CloudFront distribution.

Answer: 1, 4

Explanation:

To prevent users from circumventing the controls implemented on CloudFront (using WAF or presigned URLs / signed cookies) you can use an origin access identity (OAI). An OAI is a special CloudFront user that you associate with a distribution.

The next step is to change the permissions either on your Amazon S3 bucket or on the files in your bucket so that only the origin access identity has read permission (or read and download permission). This can be implemented through a bucket policy.

To control access at the CloudFront layer the AWS Web Application Firewall (WAF) can be used. With WAF you must create an ACL that includes the IP restrictions required and then associate the web ACL with the CloudFront distribution.

CORRECT: "Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects" is a correct answer.

CORRECT: "Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution" is also a correct answer.

INCORRECT: "Create an origin access identity (OAI) and associate it with the distribution. Generate presigned URLs that limit access to the OAI" is incorrect. Presigned URLs can be used to protect access to CloudFront but they cannot be used to limit access to an OAI.

INCORRECT: "Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the Amazon S3 bucket" is incorrect. The Web ACL should be associated with CloudFront, not S3.

INCORRECT: "Attach the existing security group that contains the IP restrictions to the Amazon CloudFront distribution" is incorrect. You cannot attach a security group to a CloudFront distribution.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-waf-and-shield/>

QUESTION 24

A company is storing a large quantity of small files in an Amazon S3 bucket. An application running on an Amazon EC2 instance needs permissions to access and process the files in the S3 bucket.

Which action will MOST securely grant the EC2 instance access to the S3 bucket?

1. Create a bucket ACL on the S3 bucket and configure the EC2 instance ID as a grantee.
2. Create an IAM role with least privilege permissions and attach it to the EC2 instance profile.
3. Create an IAM user for the application with specific permissions to the S3 bucket.
4. Generate access keys and store the credentials on the EC2 instance for use in making API calls.

Answer: 2

Explanation:

IAM roles should be used in place of storing credentials on Amazon EC2 instances. This is the most secure way to provide permissions to EC2 as no credentials are stored and short-lived credentials are obtained using AWS STS. Additionally, the policy attached to the role should provide least privilege permissions.

CORRECT: "Create an IAM role with least privilege permissions and attach it to the EC2 instance profile" is the correct answer.

INCORRECT: "Generate access keys and store the credentials on the EC2 instance for use in making API calls" is incorrect. This is not best practice, IAM roles are preferred.

INCORRECT: "Create an IAM user for the application with specific permissions to the S3 bucket" is incorrect. Instances should use IAM Roles for delegation not user accounts.

INCORRECT: "Create a bucket ACL on the S3 bucket and configure the EC2 instance ID as a grantee" is incorrect. You cannot configure an EC2 instance ID on a bucket ACL and bucket ACLs cannot be used to restrict access in this scenario.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 25

A company requires a solution to allow customers to customize images that are stored in an online catalog. The image customization parameters will be sent in requests to Amazon API Gateway. The customized image will then be generated on-demand and can be accessed online.

The solutions architect requires a highly available solution. Which solution will be MOST cost-effective?

1. Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances
2. Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin
3. Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances
4. Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin

Answer: 2

Explanation:

All solutions presented are highly available. The key requirement that must be satisfied is that the solution should be cost-effective and you must choose the most cost-effective option.

Therefore, it's best to eliminate services such as Amazon EC2 and ELB as these require ongoing costs even when they're not used. Instead, a fully serverless solution should be used. AWS Lambda, Amazon S3 and CloudFront are the best services to use for these requirements.

CORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is the correct answer.

INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances" is incorrect. This is not the most cost-effective option as the ELB and EC2 instances will incur costs even when not used.

INCORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances" is incorrect. This is not the most cost-effective option as the ELB will incur costs even when not used. Also, Amazon DynamoDB will incur RCU/WCUs when running and is not the best choice for storing images.

INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is incorrect. This is not the most cost-effective option as the EC2 instances will incur costs even when not used

References:

<https://aws.amazon.com/serverless/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 26

A solutions architect is finalizing the architecture for a distributed database that will run across multiple Amazon EC2 instances. Data will be replicated across all instances so the loss of an instance will not cause loss of data. The database requires block storage with low latency and throughput that supports up to several million transactions per second per server.

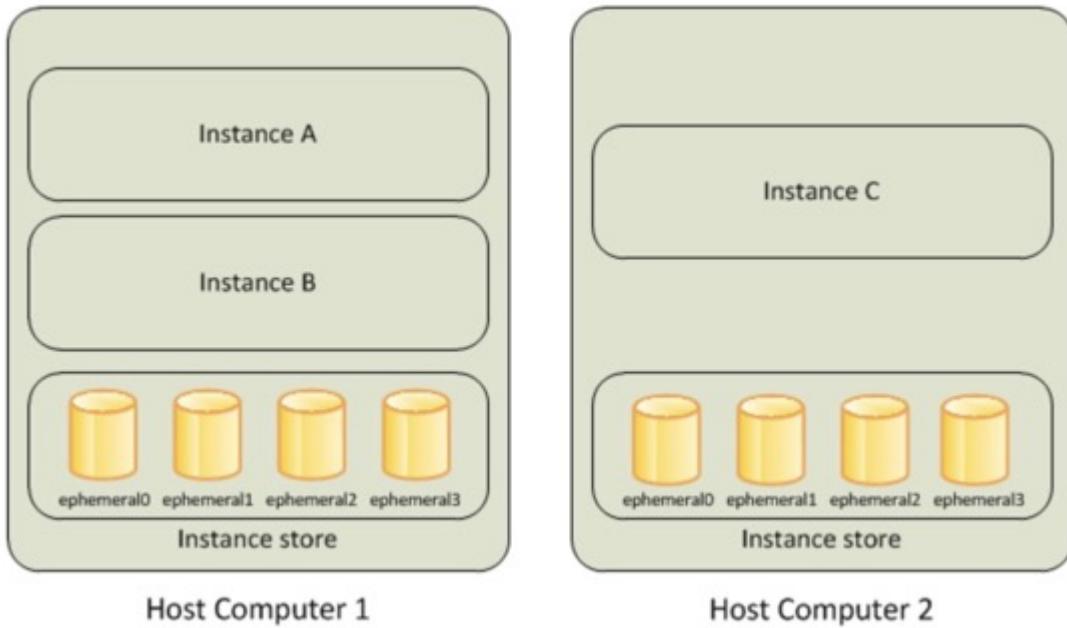
Which storage solution should the solutions architect use?

1. Amazon EBS
2. Amazon EC2 instance store
3. Amazon EFS
4. Amazon S3

Answer: 2

Explanation:

An *instance store* provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.



Some instance types use NVMe or SATA-based solid state drives (SSD) to deliver high random I/O performance. This is a good option when you need storage with very low latency, but you don't need the data to persist when the instance terminates or you can take advantage of fault-tolerant architectures.

In this scenario the data is replicated and fault tolerant so the best option to provide the level of performance required is to use instance store volumes.

CORRECT: "Amazon EC2 instance store" is the correct answer.

INCORRECT: "Amazon EBS" is incorrect. The Elastic Block Store (EBS) is a block storage device but as the data is distributed and fault tolerant a better option for performance would be to use instance stores.

INCORRECT: "Amazon EFS" is incorrect as EFS is not a block device, it is a filesystem that is accessed using the NFS protocol.

INCORRECT: "Amazon S3" is incorrect as S3 is an object-based storage system, not a block-based storage system.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 27

A website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website's DNS records are hosted in Amazon Route 53 with the domain name pointing to the ALB. A solution is required for displaying a static error page if the website becomes unavailable.

Which configuration should a solutions architect use to meet these requirements with the LEAST operational overhead?

1. Create a Route 53 alias record for an Amazon CloudFront distribution and specify the ALB as the origin. Create custom error pages for the distribution
2. Create a Route 53 active-passive failover configuration. Create a static website using an Amazon S3 bucket that hosts a static error page. Configure the static website as the passive record for failover
3. Create a Route 53 weighted routing policy. Create a static website using an Amazon S3 bucket that hosts a static error page. Configure the record for the S3 static website with a weighting of zero. When an issue occurs increase the weighting

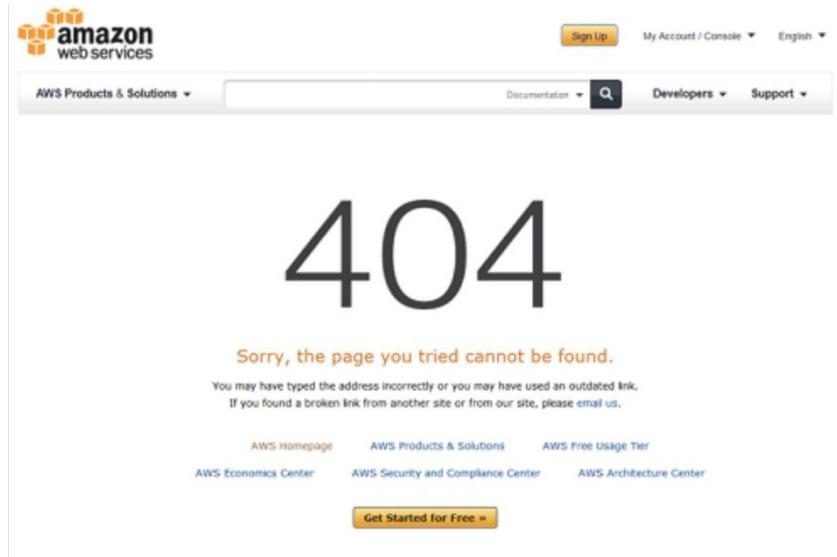
4. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB

Answer: 1

Explanation:

Using Amazon CloudFront as the front-end provides the option to specify a custom message instead of the default message. To specify the specific file that you want to return and the errors for which the file should be returned, you update your CloudFront distribution to specify those values.

For example, the following is a customized error message:



The CloudFront distribution can use the ALB as the origin, which will cause the website content to be cached on the CloudFront edge caches.

This solution represents the most operationally efficient choice as no action is required in the event of an issue, other than troubleshooting the root cause.

CORRECT: "Create a Route 53 alias record for an Amazon CloudFront distribution and specify the ALB as the origin. Create custom error pages for the distribution" is the correct answer.

INCORRECT: "Create a Route 53 active-passive failover configuration. Create a static website using an Amazon S3 bucket that hosts a static error page. Configure the static website as the passive record for failover" is incorrect. This option does not represent the lowest operational overhead as manual intervention would be required to cause a fail-back to the main website.

INCORRECT: "Create a Route 53 weighted routing policy. Create a static website using an Amazon S3 bucket that hosts a static error page. Configure the record for the S3 static website with a weighting of zero. When an issue occurs increase the weighting" is incorrect. This option requires manual intervention and there would be a delay from the issue arising before an administrative action could make the changes.

INCORRECT: "Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB" is incorrect. With an active-active configuration traffic would be split between the website and the error page.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/custom-error-pages.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 28

A company is deploying a new web application that will run on Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. The application requires a shared storage solution that offers strong consistency as the content will be regularly updated.

Which solution requires the LEAST amount of effort?

1. Create an Amazon S3 bucket to store the web content and use Amazon CloudFront to deliver the content
2. Create an Amazon Elastic File System (Amazon EFS) file system and mount it on the individual Amazon EC2 instances
3. Create a shared Amazon Block Store (Amazon EBS) volume and mount it on the individual Amazon EC2 instances
4. Create a volume gateway using AWS Storage Gateway to host the data and mount it to the Auto Scaling group

Answer: 2

Explanation:

Amazon EFS is a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud. EFS file systems are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and support full file system access semantics (such as strong consistency and file locking).

EFS is a good solution for when you need to attach a shared filesystem to multiple EC2 instances across multiple Availability Zones.

CORRECT: "Create an Amazon Elastic File System (Amazon EFS) file system and mount it on the individual Amazon EC2 instances" is the correct answer.

INCORRECT: "Create an Amazon S3 bucket to store the web content and use Amazon CloudFront to deliver the content" is incorrect as this may require more effort in terms of reprogramming the application to use the S3 API.

INCORRECT: "Create a shared Amazon Block Store (Amazon EBS) volume and mount it on the individual Amazon EC2 instances" is incorrect. Please note that you can multi-attach an EBS volume to multiple EC2 instances but the instances must be in the same AZ.

INCORRECT: "Create a volume gateway using AWS Storage Gateway to host the data and mount it to the Auto Scaling group" is incorrect as a storage gateway is used on-premises.

References:

<https://aws.amazon.com/efs/faq/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 29

A web application has recently been launched on AWS. The architecture includes two tier with a web layer and a database layer. It has been identified that the web server layer may be vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

1. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF
2. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF
3. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF
4. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard

Answer: 3

Explanation:

The AWS Web Application Firewall (WAF) is available on the Application Load Balancer (ALB). You can use AWS WAF directly on Application Load Balancers (both internal and external) in a VPC, to protect your websites and web services.

Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF to inspect for possible malicious scripts.

CORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is the correct answer.

INCORRECT: "Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a classic load balancer.

INCORRECT: "Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a network load balancer.

INCORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard" is incorrect as you cannot use AWS Shield to protect against XSS attacks. Shield is used to protect against DDoS attacks.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-waf-and-shield/>

QUESTION 30

A multi-tier application runs with eight front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer. A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

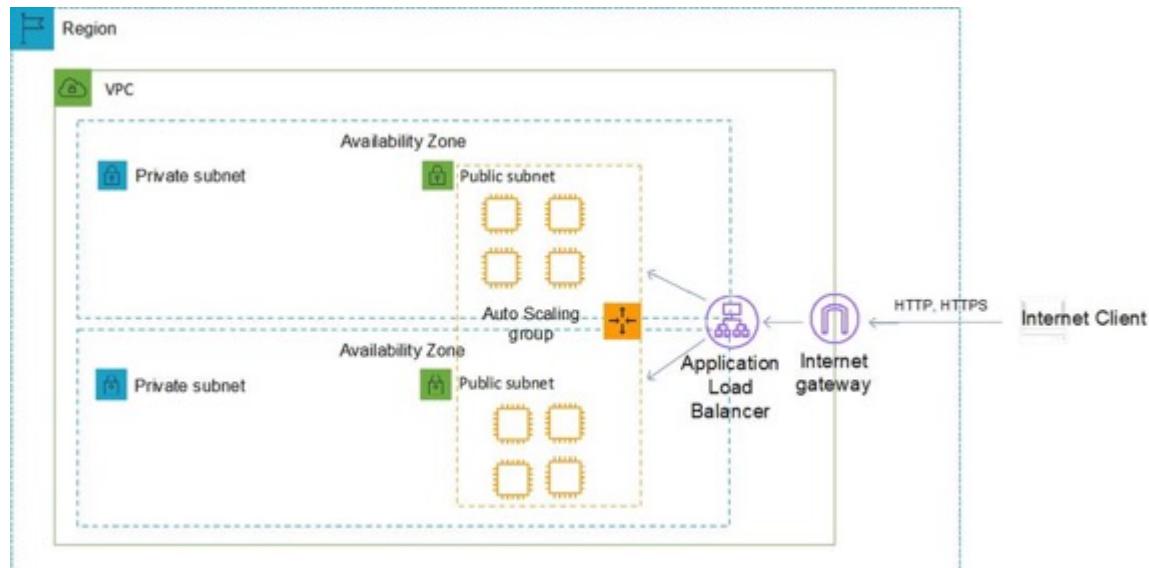
1. Create an Auto Scaling group that uses four instances across each of two Regions
2. Modify the Auto Scaling group to use four instances across each of two Availability Zones
3. Create an Auto Scaling template that can be used to quickly create more instances in another Region
4. Create an Auto Scaling group that uses four instances across each of two subnets

Answer: 2

Explanation:

High availability can be enabled for this architecture quite simply by modifying the existing Auto Scaling group to use multiple availability zones. The ASG will automatically balance the load so you don't actually need to specify the instances per AZ.

The architecture for the web tier will look like the one below:



CORRECT: "Modify the Auto Scaling group to use four instances across each of two Availability Zones" is the correct answer.

INCORRECT: "Create an Auto Scaling group that uses four instances across each of two Regions" is incorrect as EC2 Auto Scaling does not support multiple regions.

INCORRECT: "Create an Auto Scaling template that can be used to quickly create more instances in another Region" is incorrect

as EC2 Auto Scaling does not support multiple regions.

INCORRECT: "Create an Auto Scaling group that uses four instances across each of two subnets" is incorrect as the subnets could be in the same AZ.

References:

<https://aws.amazon.com/ec2/autoscaling/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 31

A company's web application is using multiple Amazon EC2 Linux instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure.

What should a solutions architect do to meet these requirements?

1. Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance
2. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance
3. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance
4. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-A)

Answer: 3

Explanation:

To increase the resiliency of the application the solutions architect can use Auto Scaling groups to launch and terminate instances across multiple availability zones based on demand. An application load balancer (ALB) can be used to direct traffic to the web application running on the EC2 instances.

Lastly, the Amazon Elastic File System (EFS) can assist with increasing the resilience of the application by providing a shared file system that can be mounted by multiple EC2 instances from multiple availability zones.

CORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance" is the correct answer.

INCORRECT: "Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance" is incorrect as the EBS volumes are single points of failure which are not shared with other instances.

INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance" is incorrect as instance stores are ephemeral data stores which means data is lost when powered down. Also, instance stores cannot be shared between instances.

INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as there are data retrieval charges associated with this S3 tier. It is not a suitable storage tier for application files.

References:

<https://docs.aws.amazon.com/efs/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 32

A website runs on a Microsoft Windows server in an on-premises data center. The web server is being migrated to Amazon EC2 Windows instances in multiple Availability Zones on AWS. The web server currently uses data stored in an on-premises network-attached storage (NAS) device.

Which replacement to the NAS file share is MOST resilient and durable?

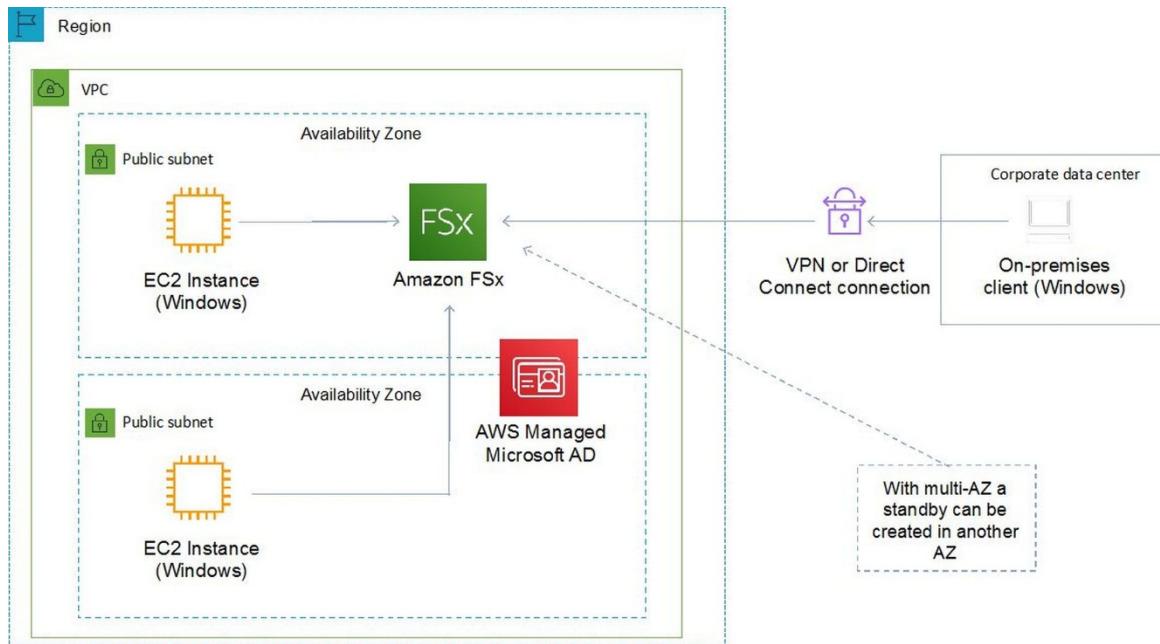
1. Migrate the file share to Amazon EBS
2. Migrate the file share to AWS Storage Gateway

3. Migrate the file share to Amazon FSx for Windows File Server
4. Migrate the file share to Amazon Elastic File System (Amazon EFS)

Answer: 3

Explanation:

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit.



This is the only solution presented that provides resilient storage for Windows instances.

CORRECT: "Migrate the file share to Amazon FSx for Windows File Server" is the correct answer.

INCORRECT: "Migrate the file share to Amazon Elastic File System (Amazon EFS)" is incorrect as you cannot use Windows instances with Amazon EFS.

INCORRECT: "Migrate the file share to Amazon EBS" is incorrect as this is not a shared storage solution for multi-AZ deployments.

INCORRECT: "Migrate the file share to AWS Storage Gateway" is incorrect as with Storage Gateway replicated files end up on Amazon S3. The replacement storage solution should be a file share, not an object-based storage system.

References:

<https://aws.amazon.com/fsx/windows/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 33

A company is planning a migration for a high performance computing (HPC) application and associated data from an on-premises data center to the AWS Cloud. The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.

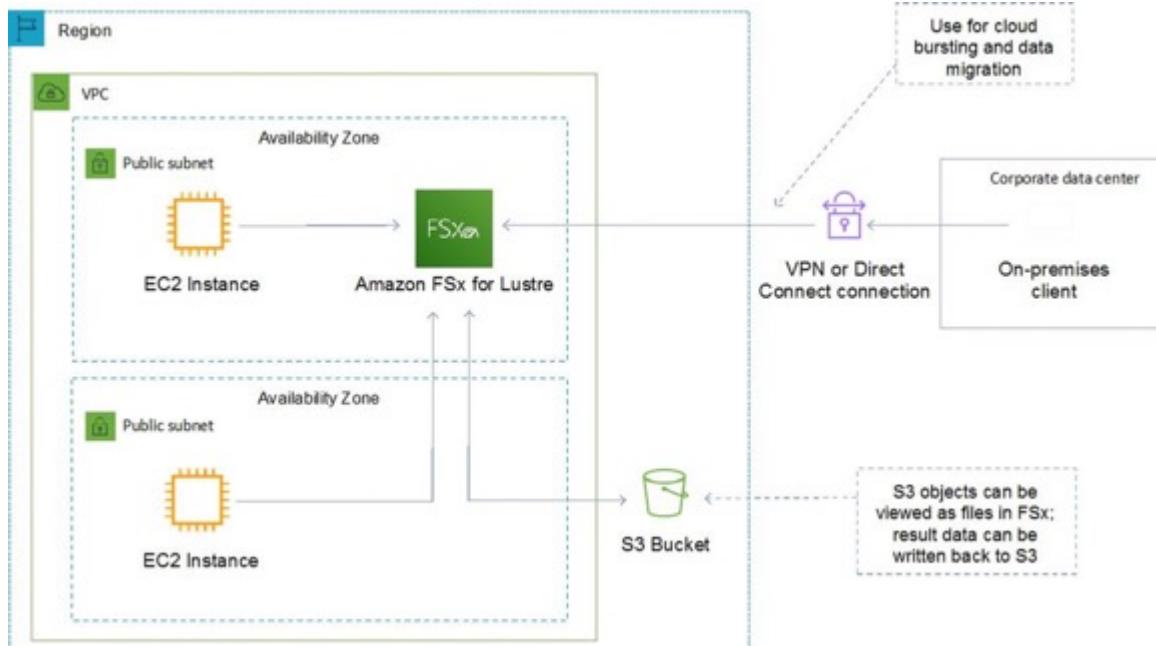
Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO.)

1. Amazon S3 for cold data storage
2. Amazon EFS for cold data storage
3. Amazon S3 for high-performance parallel storage
4. Amazon FSx for Lustre for high-performance parallel storage
5. Amazon FSx for Windows for high-performance parallel storage

Answer: 1,4

Explanation:

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA). These workloads commonly require data to be presented via a fast and scalable file system interface, and typically have data sets stored on long-term data stores like Amazon S3.



Amazon FSx works natively with Amazon S3, making it easy to access your S3 data to run data processing workloads. Your S3 objects are presented as files in your file system, and you can write your results back to S3. This lets you run data processing workloads on FSx for Lustre and store your long-term data on S3 or on-premises data stores.

Therefore, the best combination for this scenario is to use S3 for cold data storage and FSx for Lustre for the parallel HPC job.

CORRECT: "Amazon S3 for cold data storage" is the correct answer.

CORRECT: "Amazon FSx for Lustre for high-performance parallel storage" is the correct answer.

INCORRECT: "Amazon EFS for cold data storage" is incorrect as FSx works natively with S3 which is also more economical.

INCORRECT: "Amazon S3 for high-performance parallel storage" is incorrect as S3 is not suitable for running high-performance computing jobs.

INCORRECT: "Amazon FSx for Windows for high-performance parallel storage" is incorrect as FSx for Lustre should be used for HPC use cases and use cases that require storing data on S3.

References:

<https://aws.amazon.com/fsx/lustre/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 34

A web application that allows users to upload and share documents is running on a single Amazon EC2 instance with an Amazon EBS volume. To increase availability the architecture has been updated to use an Auto Scaling group of several instances across Availability Zones behind an Application Load Balancer. After the change users can only see a subset of the documents.

What is the BEST method for a solutions architect to modify the solution so users can see all documents?

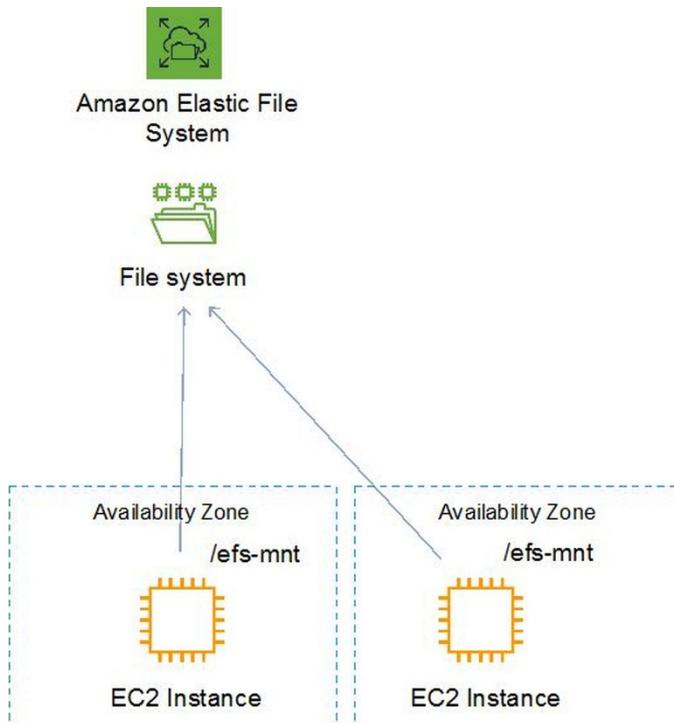
1. Run a script to synchronize the data between Amazon EBS volumes
2. Use Sticky Sessions with the ALB to ensure users are directed to the same EC2 instance in a session
3. Copy the data from all EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS
4. Configure the Application Load Balancer to send the request to all servers. Return each document from the correct server

Answer: 3

Explanation:

The problem that is being described is that the users are uploading the documents to an individual EC2 instance with a local EBS volume. Therefore, as EBS volumes cannot be shared across AZs, the data is stored separately and the ALB will be distributing incoming connections to different instances / data sets.

The simple resolution is to implement a shared storage layer for the documents so that they can be stored in one place and seen by any user who connects no matter which instance they connect to.



CORRECT: "Copy the data from all EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS" is the correct answer.

INCORRECT: "Run a script to synchronize the data between Amazon EBS volumes" is incorrect. This is a complex and messy approach. A better solution is to use a shared storage layer.

INCORRECT: "Use Sticky Sessions with the ALB to ensure users are directed to the same EC2 instance in a session" is incorrect as this will just "stick" a user to the same instance. They won't see documents uploaded to other instances / EBS volumes.

INCORRECT: "Configure the Application Load Balancer to send the request to all servers. Return each document from the correct server" is incorrect as there is no mechanism here for selecting a specific document. The requirement also requests that all documents are visible.

References:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 35

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 midmorning

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

1. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens
2. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period
3. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period
4. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens

Answer: 3

Explanation:

Though this sounds like a good use case for scheduled actions, both answers using scheduled actions will have 20 instances running regardless of actual demand. A better option to be more cost effective is to use a target tracking action that triggers at a lower CPU threshold.

With this solution the scaling will occur before the CPU utilization gets to a point where performance is affected. This will result in resolving the performance issues whilst minimizing costs. Using a reduced cooldown period will also more quickly terminate unneeded instances, further reducing costs.

CORRECT: "Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period" is the correct answer.

INCORRECT: "Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens" is incorrect as this is not the most cost-effective option. Note you can choose min, max, or desired for a scheduled action.

INCORRECT: "Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens" is incorrect as this is not the most cost-effective option. Note you can choose min, max, or desired for a scheduled action.

INCORRECT: "Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period" is incorrect as AWS recommend you use target tracking in place of step scaling for most use cases.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 36

An application uses Amazon EC2 instances and an Amazon RDS MySQL database. The database is not currently encrypted. A solutions architect needs to apply encryption to the database for all new and existing data.

How should this be accomplished?

1. Create an Amazon ElastiCache cluster and encrypt data using the cache nodes
2. Enable encryption for the database using the API. Take a full snapshot of the database. Delete old snapshots
3. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot
4. 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: 3

Explanation:

There are some [limitations for encrypted Amazon RDS DB Instances](#): you can't modify an existing unencrypted Amazon RDS DB instance to make the instance encrypted, and you can't create an encrypted read replica from an unencrypted instance.

However, you can use the Amazon RDS snapshot feature to encrypt an unencrypted snapshot that's taken from the RDS database that you want to encrypt. Restore a new RDS DB instance from the encrypted snapshot to deploy a new encrypted DB instance. Finally, switch your connections to the new DB instance.

CORRECT: "Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot" is the correct answer.

INCORRECT: "Create an Amazon ElastiCache cluster and encrypt data using the cache nodes" is incorrect as you cannot encrypt an RDS database using an ElastiCache cache node.

INCORRECT: "Enable encryption for the database using the API. Take a full snapshot of the database. Delete old snapshots" is incorrect as you cannot enable encryption for an existing database.

INCORRECT: "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" is incorrect as you cannot create an encrypted read replica from an unencrypted database instance.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/rds-encrypt-instance-mysql-mariadb/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 37

A company have 500 TB of data in an on-premises file share that needs to be moved to Amazon S3 Glacier. The migration must not saturate the company's low-bandwidth internet connection and the migration must be completed within a few weeks.

What is the MOST cost-effective solution?

1. Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier
2. Order 7 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint
3. Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth
4. Order 7 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier

Answer: 4

Explanation:

As the company's internet link is low-bandwidth uploading directly to Amazon S3 (ready for transition to Glacier) would saturate the link. The best alternative is to use AWS Snowball appliances. The Snowball edge appliance can hold up to 80 TB of data so 7 devices would be required to migrate 500 TB of data.

Snowball moves data into AWS using a hardware device and the data is then copied into an Amazon S3 bucket of your choice. From there, lifecycle policies can transition the S3 objects to Amazon S3 Glacier.

CORRECT: "Order 7 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier" is the correct answer.

INCORRECT: "Order 7 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint" is incorrect as you cannot set a Glacier vault as the destination, it must be an S3 bucket. You also can't enforce a VPC endpoint using a bucket policy.

INCORRECT: "Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier" is incorrect as this is not the most cost-effective option and takes time to setup.

INCORRECT: "Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth" is incorrect as this service is not used for accelerating or optimizing the upload of data from on-premises networks.

References:

<https://docs.aws.amazon.com/snowball/latest/developer-guide/specifications.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 38

A company has refactored a legacy application to run as two microservices using Amazon ECS. The application processes data in two parts and the second part of the process takes longer than the first.

How can a solutions architect integrate the microservices and allow them to scale independently?

1. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2
2. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic
3. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose
4. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue

Answer: 4

Explanation:

This is a good use case for Amazon SQS. The microservices must be decoupled so they can scale independently. An Amazon SQS queue will enable microservice 1 to add messages to the queue. Microservice 2 can then pick up the messages and process them. This ensures that if there's a spike in traffic on the frontend, messages do not get lost due to the backend process not being ready to process them.

CORRECT: "Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue" is the correct answer.

INCORRECT: "Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2" is incorrect as a message queue would be preferable to an S3 bucket.

INCORRECT: "Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic" is incorrect as notifications to topics are pushed to subscribers. In this case we want the second microservice to pickup the messages when ready (pull them).

INCORRECT: "Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose" is incorrect as this is not how Firehose works. Firehose sends data directly to destinations, it is not a message queue.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 39

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.)

1. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0
2. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0
3. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier
4. 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

5. 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: 1, 3

Explanation:

In this scenario an inbound rule is required to allow traffic from any internet client to the web front end on SSL/TLS port 443. The source should therefore be set to 0.0.0.0/0 to allow any inbound traffic.

To secure the connection from the web frontend to the database tier, an outbound rule should be created from the public EC2 security group with a destination of the private EC2 security group. The port should be set to 1433 for MySQL. The private EC2 security group will also need to allow inbound traffic on 1433 from the public EC2 security group.

This configuration can be seen in the diagram:



CORRECT: "Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0" is a correct answer.

CORRECT: "Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier" is also a correct answer.

INCORRECT: "Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0" is incorrect as this is configured backwards.

INCORRECT: "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" is incorrect as the MySQL database instance does not need to send outbound traffic on either of these ports.

INCORRECT: "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" is incorrect as the database tier does not need to allow inbound traffic on port 443.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon->

QUESTION 40

A solutions architect has created a new AWS account and must secure AWS account root user access.

Which combination of actions will accomplish this? (Select TWO.)

1. Ensure the root user uses a strong password
2. Enable multi-factor authentication to the root user
3. Store root user access keys in an encrypted Amazon S3 bucket
4. Add the root user to a group containing administrative permissions
5. Delete the root user account

Answer: 1, 2

Explanation:

There are several security best practices for securing the root user account:

- Lock away root user access keys OR delete them if possible
- Use a strong password
- Enable multi-factor authentication (MFA)

The root user automatically has full privileges to the account and these privileges cannot be restricted so it is extremely important to follow best practice advice about securing the root user account.

CORRECT: "Ensure the root user uses a strong password" is the correct answer.

CORRECT: "Enable multi-factor authentication to the root user" is the correct answer.

INCORRECT: "Store root user access keys in an encrypted Amazon S3 bucket" is incorrect as the best practice is to lock away or delete the root user access keys. An S3 bucket is not a suitable location for storing them, even if encrypted.

INCORRECT: "Add the root user to a group containing administrative permissions" is incorrect as this does not restrict access and is unnecessary.

INCORRECT: "Delete the root user account" is incorrect as you cannot delete the root user account.

References:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 41

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.

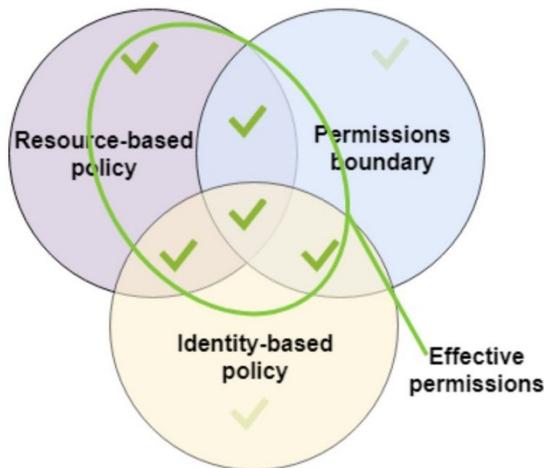
How should a solutions architect address this issue?

1. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
2. Use service control policies to disable IAM activity across all accounts in the organizational unit
3. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
4. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Answer: 4

Explanation:

The permissions boundary for an IAM entity (user or role) sets the maximum permissions that the entity can have. This can change the effective permissions for that user or role. The effective permissions for an entity are the permissions that are granted by all the policies that affect the user or role. Within an account, the permissions for an entity can be affected by identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, or session policies.



Therefore, the solutions architect can set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

CORRECT: "Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy" is the correct answer.

INCORRECT: "Create an Amazon SNS topic to send an alert every time a developer creates a new policy" is incorrect as this would mean investigating every incident which is not an efficient solution.

INCORRECT: "Use service control policies to disable IAM activity across all accounts in the organizational unit" is incorrect as this would prevent the developers from being able to work with IAM completely.

INCORRECT: "Prevent the developers from attaching any policies and assign all IAM duties to the security operations team" is incorrect as this is not necessary. The requirement is to allow developers to work with policies, the solution needs to find a secure way of achieving this.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 42

A solutions architect is optimizing a website for real-time streaming and on-demand videos. The website's users are located around the world and the solutions architect needs to optimize the performance for both the real-time and on-demand streaming.

Which service should the solutions architect choose?

1. Amazon CloudFront
2. AWS Global Accelerator
3. Amazon Route 53
4. Amazon S3 Transfer Acceleration

Answer: 1

Explanation:

Amazon CloudFront can be used to stream video to users across the globe using a wide variety of protocols that are layered on top of HTTP. This can include both on-demand video as well as real time streaming video.

CORRECT: "Amazon CloudFront" is the correct answer.

INCORRECT: "AWS Global Accelerator" is incorrect as this would be an expensive way of getting the content closer to users

compared to using CloudFront. As this is a use case for CloudFront and there are so many edge locations it is the better option.

INCORRECT: "Amazon Route 53" is incorrect as you still need a solution for getting the content closer to users.

INCORRECT: "Amazon S3 Transfer Acceleration" is incorrect as this is used to accelerate uploads of data to Amazon S3 buckets.

References:

<https://aws.amazon.com/cloudfront/streaming/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 43

Objects uploaded to Amazon S3 are initially accessed frequently for a period of 30 days. Then, objects are infrequently accessed for up to 90 days. After that, the objects are no longer needed.

How should lifecycle management be configured?

1. Transition to STANDARD_IA after 30 days. After 90 days transition to GLACIER
2. Transition to STANDARD_IA after 30 days. After 90 days transition to ONEZONE_IA
3. Transition to ONEZONE_IA after 30 days. After 90 days expire the objects
4. Transition to REDUCED_REDUNDANCY after 30 days. After 90 days expire the objects

Answer: 3

Explanation:

In this scenario we need to keep the objects in the STANDARD storage class for 30 days as the objects are being frequently accessed. We can configure a lifecycle action that then transitions the objects to INTELLIGENT_TIERING, STANDARD_IA, or ONEZONE_IA. After that we don't need the objects so they can be expired.

All other options do not meet the stated requirements or are not supported lifecycle transitions. For example:

- You cannot transition to REDUCED_REDUNDANCY from any storage class.
- Transitioning from STANDARD_IA to ONEZONE_IA is possible but we do not want to keep the objects so it incurs unnecessary costs.
- Transitioning to GLACIER is possible but again incurs unnecessary costs.

CORRECT: "Transition to ONEZONE_IA after 30 days. After 90 days expire the objects " is the correct answer.

INCORRECT: "Transition to STANDARD_IA after 30 days. After 90 days transition to GLACIER" is incorrect.

INCORRECT: "Transition to STANDARD_IA after 30 days. After 90 days transition to ONEZONE_IA" is incorrect.

INCORRECT: "Transition to REDUCED_REDUNDANCY after 30 days. After 90 days expire the objects " is incorrect.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 44

A company has acquired another business and needs to migrate their 50TB of data into AWS within 1 month. They also require a secure, reliable and private connection to the AWS cloud.

How are these requirements best accomplished?

1. Provision an AWS Direct Connect connection and migrate the data over the link
2. Migrate data using AWS Snowball. Provision an AWS VPN initially and order a Direct Connect link
3. Launch a Virtual Private Gateway (VPG) and migrate the data over the AWS VPN
4. Provision an AWS VPN CloudHub connection and migrate the data over redundant links

Answer: 2

Explanation:

AWS Direct Connect provides a secure, reliable and private connection. However, lead times are often longer than 1 month so it cannot be used to migrate data within the timeframes. Therefore, it is better to use AWS Snowball to move the data and order a Direct Connect connection to satisfy the other requirement later on. In the meantime the organization can use an AWS VPN for secure, private access to their VPC.

CORRECT: "Migrate data using AWS Snowball. Provision an AWS VPN initially and order a Direct Connect link" is the correct answer.

INCORRECT: "Provision an AWS Direct Connect connection and migrate the data over the link" is incorrect due to the lead time for installation.

INCORRECT: "Launch a Virtual Private Gateway (VPG) and migrate the data over the AWS VPN" is incorrect. A VPG is the AWS-side of an AWS VPN. A VPN does not provide a private connection and is not reliable as you can never guarantee the latency over the Internet

INCORRECT: "Provision an AWS VPN CloudHub connection and migrate the data over redundant links" is incorrect. AWS VPN CloudHub is a service for connecting multiple sites into your VPC over VPN connections. It is not used for aggregating links and the limitations of Internet bandwidth from the company where the data is stored will still be an issue. It also uses the public Internet so is not a private or reliable connection.

References:

<https://aws.amazon.com/snowball/>

<https://aws.amazon.com/directconnect/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-snowball/>

QUESTION 45

An application on Amazon Elastic Container Service (ECS) performs data processing in two parts. The second part takes much longer to complete. How can an Architect decouple the data processing from the backend application component?

1. Process both parts using the same ECS task. Create an Amazon Kinesis Firehose stream
2. Process each part using a separate ECS task. Create an Amazon SNS topic and send a notification when the processing completes
3. Create an Amazon DynamoDB table and save the output of the first part to the table
4. Process each part using a separate ECS task. Create an Amazon SQS queue

Answer: 4

Explanation:

Processing each part using a separate ECS task may not be essential but means you can separate the processing of the data. An Amazon Simple Queue Service (SQS) is used for decoupling applications. It is a message queue on which you place messages for processing by application components. In this case you can process each data processing part in separate ECS tasks and have them write an Amazon SQS queue. That way the backend can pick up the messages from the queue when they're ready and there is no delay due to the second part not being complete.

CORRECT: "Process each part using a separate ECS task. Create an Amazon SQS queue" is the correct answer.

INCORRECT: "Process both parts using the same ECS task. Create an Amazon Kinesis Firehose stream" is incorrect. Amazon Kinesis Firehose is used for streaming data. This is not an example of streaming data. In this case SQS is better as a message can be placed on a queue to indicate that the job is complete and ready to be picked up by the backend application component.

INCORRECT: "Process each part using a separate ECS task. Create an Amazon SNS topic and send a notification when the processing completes" is incorrect. Amazon Simple Notification Service (SNS) can be used for sending notifications. It is useful when you need to notify multiple AWS services. In this case an Amazon SQS queue is a better solution as there is no mention of multiple AWS services and this is an ideal use case for SQS.

INCORRECT: "Create an Amazon DynamoDB table and save the output of the first part to the table" is incorrect. Amazon DynamoDB is unlikely to be a good solution for this requirement. There is a limit on the maximum amount of data that you can

store in an entry in a DynamoDB table.

References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 46

An application is running on Amazon EC2 behind an Elastic Load Balancer (ELB). Content is being published using Amazon CloudFront and you need to restrict the ability for users to circumvent CloudFront and access the content directly through the ELB.

How can you configure this solution?

1. Create an Origin Access Identity (OAI) and associate it with the distribution
2. Use signed URLs or signed cookies to limit access to the content
3. Use a Network ACL to restrict access to the ELB
4. Create a VPC Security Group for the ELB and use AWS Lambda to automatically update the CloudFront internal service IP addresses when they change

Answer: 4

Explanation:

The only way to get this working is by using a VPC Security Group for the ELB that is configured to allow only the internal service IP ranges associated with CloudFront. As these are updated from time to time, you can use AWS Lambda to automatically update the addresses. This is done using a trigger that is triggered when AWS issues an SNS topic update when the addresses are changed.

CORRECT: "Create a VPC Security Group for the ELB and use AWS Lambda to automatically update the CloudFront internal service IP addresses when they change" is the correct answer.

INCORRECT: "Create an Origin Access Identity (OAI) and associate it with the distribution" is incorrect. You can use an OAI to restrict access to content in Amazon S3 but not on EC2 or ELB.

INCORRECT: "Use signed URLs or signed cookies to limit access to the content" is incorrect. Signed cookies and URLs are used to limit access to files but this does not stop people from circumventing CloudFront and accessing the ELB directly.

INCORRECT: "Use a Network ACL to restrict access to the ELB" is incorrect. A Network ACL can be used to restrict access to an ELB but it is recommended to use security groups and this solution is incomplete as it does not account for the fact that the internal service IP ranges change over time.

References:

<https://aws.amazon.com/blogs/security/how-to-automatically-update-your-security-groups-for-amazon-cloudfront-and-aws-waf-by-using-aws-lambda/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 47

A company has divested a single business unit and needs to move the AWS account owned by the business unit to another AWS Organization. How can this be achieved?

1. Create a new account in the destination AWS Organization and migrate resources
2. Create a new account in the destination AWS Organization and share the original resources using AWS Resource Access Manager
3. Migrate the account using AWS CloudFormation
4. Migrate the account using the AWS Organizations console

Answer: 4

Explanation:

Accounts can be migrated between organizations. To do this you must have root or IAM access to both the member and master accounts. Resources will remain under the control of the migrated account.

CORRECT: "Migrate the account using the AWS Organizations console" is the correct answer.

INCORRECT: "Create a new account in the destination AWS Organization and migrate resources" is incorrect. You do not need to create a new account in the destination AWS Organization as you can just migrate the existing account.

INCORRECT: "Create a new account in the destination AWS Organization and share the original resources using AWS Resource Access Manager" is incorrect. You do not need to create a new account in the destination AWS Organization as you can just migrate the existing account.

INCORRECT: "Migrate the account using AWS CloudFormation" is incorrect. You do not need to use AWS CloudFormation. You can use the Organizations API or AWS CLI for when there are many accounts to migrate and therefore you could use CloudFormation for any additional automation but it is not necessary for this scenario.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/organizations-move-accounts/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-organizations/>

QUESTION 48

An Amazon RDS PostgreSQL database is configured as Multi-AZ. A solutions architect needs to scale read performance and the solution must be configured for high availability. What is the most cost-effective solution?

1. Create a read replica as a Multi-AZ DB instance
2. Deploy a read replica in a different AZ to the master DB instance
3. Deploy a read replica using Amazon ElastiCache
4. Deploy a read replica in the same AZ as the master DB instance

Answer: 1

Explanation:

You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

CORRECT: "Create a read replica as a Multi-AZ DB instance" is the correct answer.

INCORRECT: "Deploy a read replica in a different AZ to the master DB instance" is incorrect as this does not provide high availability for the read replica

INCORRECT: "Deploy a read replica using Amazon ElastiCache" is incorrect as ElastiCache is not used to create read replicas of RDS database.

INCORRECT: "Deploy a read replica in the same AZ as the master DB instance" is incorrect as this solution does not include HA for the read replica.

References:

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 49

A High Performance Computing (HPC) application will be migrated to AWS. The application requires low network latency and high throughput between nodes and will be deployed in a single AZ.

How should the application be deployed for best inter-node performance?

1. In a partition placement group
2. In a cluster placement group
3. In a spread placement group

4. Behind a Network Load Balancer (NLB)

Answer: 2

Explanation:

A cluster placement group provides low latency and high throughput for instances deployed in a single AZ. It is the best way to provide the performance required for this application.

CORRECT: "In a cluster placement group" is the correct answer.

INCORRECT: "In a partition placement group" is incorrect. A partition placement group is used for grouping instances into logical segments. It provides control and visibility into instance placement but is not the best option for performance.

INCORRECT: "In a spread placement group" is incorrect. A spread placement group is used to spread instances across underlying hardware. It is not the best option for performance.

INCORRECT: "Behind a Network Load Balancer (NLB)" is incorrect. A network load balancer is used for distributing incoming connections, this does assist with inter-node performance.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 50

A web application is deployed in multiple regions behind an ELB Application Load Balancer. You need deterministic routing to the closest region and automatic failover. Traffic should traverse the AWS global network for consistent performance.

How can this be achieved?

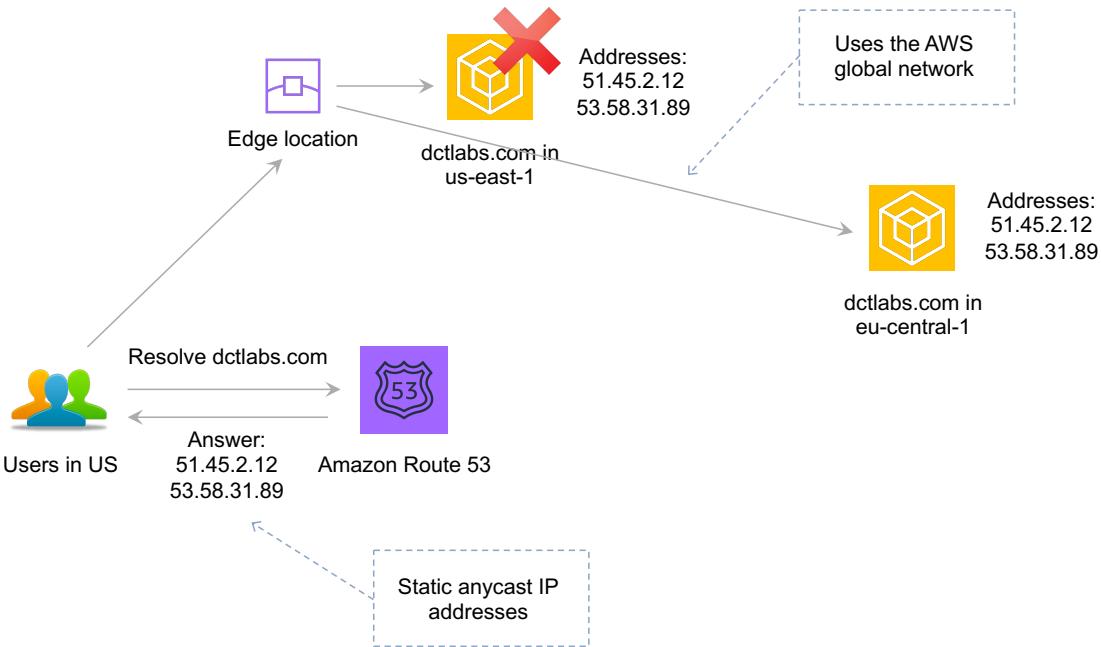
1. Configure AWS Global Accelerator and configure the ALBs as targets
2. Place an EC2 Proxy in front of the ALB and configure automatic failover
3. Create a Route 53 Alias record for each ALB and configure a latency-based routing policy
4. Use a CloudFront distribution with multiple custom origins in each region and configure for high availability

Answer: 1

Explanation:

AWS Global Accelerator is a service that improves the availability and performance of applications with local or global users. You can configure the ALB as a target and Global Accelerator will automatically route users to the closest point of presence.

Failover is automatic and does not rely on any client side cache changes as the IP addresses for Global Accelerator are static anycast addresses. Global Accelerator also uses the AWS global network which ensures consistent performance.



CORRECT: "Configure AWS Global Accelerator and configure the ALBs as targets" is the correct answer.

INCORRECT: "Place an EC2 Proxy in front of the ALB and configure automatic failover" is incorrect. Placing an EC2 proxy in front of the ALB does not meet the requirements. This solution does not ensure deterministic routing the closest region and failover is happening within a region which does not protect against regional failure. Also, this introduces a potential bottleneck and lack of redundancy.

INCORRECT: "Create a Route 53 Alias record for each ALB and configure a latency-based routing policy" is incorrect. A Route 53 Alias record for each ALB with latency-based routing does provide routing based on latency and failover. However, the traffic will not traverse the AWS global network.

INCORRECT: "Use a CloudFront distribution with multiple custom origins in each region and configure for high availability" is incorrect. You can use CloudFront with multiple custom origins and configure for HA. However, the traffic will not traverse the AWS global network.

References:

<https://aws.amazon.com/global-accelerator/>

<https://aws.amazon.com/global-accelerator/faqs/>

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-global-accelerator/>

QUESTION 51

A company's Amazon EC2 instances were terminated or stopped, resulting in a loss of important data that was stored on attached EC2 instance stores. They want to avoid this happening in the future and need a solution that can scale as data volumes increase with the LEAST amount of management and configuration.

Which storage is most appropriate?

1. Amazon EFS
2. Amazon S3
3. Amazon EBS
4. Amazon RDS

Answer: 1

Explanation:

Amazon EFS is a fully managed service that requires no changes to your existing applications and tools, providing access through a standard file system interface for seamless integration. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files. This is an easy solution to implement and the option that requires the least management and configuration.

An instance store provides temporary block-level storage for an EC2 instance. If you terminate the instance you lose all data. The alternative is to use Elastic Block Store volumes which are also block-level storage devices but the data is persistent. However, EBS is not a fully managed solution and doesn't grow automatically as your data requirements increase – you would need to increase the volume size and then extend your filesystem.

CORRECT: "Amazon EFS" is the correct answer.

INCORRECT: "Amazon S3" is incorrect. Amazon S3 is an object storage solution and as the data is currently sitting on a block storage you would need to develop some way to use the REST API to upload/manage data on S3 – this is not the easiest solution to implement.

INCORRECT: "Amazon EBS" is incorrect as EBS is not a fully managed solution and doesn't grow automatically as your data requirements increase – you would need to increase the volume size and then extend your filesystem.

INCORRECT: "Amazon RDS" is incorrect. Amazon RDS is a relational database service, the question is not looking for a database, just a way of storing data.

References:

<https://aws.amazon.com/efs/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 52

An application launched on Amazon EC2 instances needs to publish personally identifiable information (PII) about customers using Amazon SNS. The application is launched in private subnets within an Amazon VPC.

Which is the MOST secure way to allow the application to access service endpoints in the same region?

1. Use an Internet Gateway
2. Use AWS PrivateLink
3. Use a proxy instance
4. Use a NAT gateway

Answer: 2

Explanation:

To publish messages to Amazon SNS topics from an Amazon VPC, create an interface VPC endpoint. Then, you can publish messages to SNS topics while keeping the traffic within the network that you manage with the VPC. This is the most secure option as traffic does not need to traverse the Internet.

CORRECT: "Use AWS PrivateLink" is the correct answer.

INCORRECT: "Use an Internet Gateway" is incorrect. Internet Gateways are used by instances in public subnets to access the Internet and this is less secure than an VPC endpoint.

INCORRECT: "Use a proxy instance" is incorrect. A proxy instance will also use the public Internet and so is less secure than a VPC endpoint.

INCORRECT: "Use a NAT gateway" is incorrect. A NAT Gateway is used by instances in private subnets to access the Internet and this is less secure than an VPC endpoint.

References:

<https://docs.aws.amazon.com/sns/latest/dg/sns-vpc-endpoint.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 53

A Solutions Architect is designing a web application that runs on Amazon EC2 instances behind an Elastic Load Balancer. All data in transit must be encrypted.

Which solution options meet the encryption requirement? (Select TWO.)

1. Use a Network Load Balancer (NLB) with a TCP listener, then terminate SSL on EC2 instances
2. Use an Application Load Balancer (ALB) with an HTTPS listener, then install SSL certificates on the ALB and EC2 instances
3. Use an Application Load Balancer (ALB) in passthrough mode, then terminate SSL on EC2 instances
4. Use a Network Load Balancer (NLB) with an HTTPS listener, then install SSL certificates on the NLB and EC2 instances
5. Use an Application Load Balancer (ALB) with a TCP listener, then terminate SSL on EC2 instances

Answer: 1,2

Explanation:

You can passthrough encrypted traffic with an NLB and terminate the SSL on the EC2 instances, so this is a valid answer.

You can use a HTTPS listener with an ALB and install certificates on both the ALB and EC2 instances. This does not use passthrough, instead it will terminate the first SSL connection on the ALB and then re-encrypt the traffic and connect to the EC2 instances.

CORRECT: "Use a Network Load Balancer (NLB) with a TCP listener, then terminate SSL on EC2 instances" is the correct answer.

CORRECT: "Use an Application Load Balancer (ALB) with an HTTPS listener, then install SSL certificates on the ALB and EC2 instances" is the correct answer.

INCORRECT: "Use an Application Load Balancer (ALB) in passthrough mode, then terminate SSL on EC2 instances" is incorrect. You cannot use passthrough mode with an ALB and terminate SSL on the EC2 instances.

INCORRECT: "Use a Network Load Balancer (NLB) with an HTTPS listener, then install SSL certificates on the NLB and EC2 instances" is incorrect. You cannot use a HTTPS listener with an NLB.

INCORRECT: "Use an Application Load Balancer (ALB) with a TCP listener, then terminate SSL on EC2 instances" is incorrect. You cannot use a TCP listener with an ALB.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 54

An application running video-editing software is using significant memory on an Amazon EC2 instance. How can a user track memory usage on the Amazon EC2 instance?

1. Install the CloudWatch agent on the EC2 instance to push memory usage to an Amazon CloudWatch custom metric
2. Use an instance type that supports memory usage reporting to a metric by default
3. Call Amazon CloudWatch to retrieve the memory usage metric data that exists for the EC2 instance
4. Assign an IAM role to the EC2 instance with an IAM policy granting access to the desired metric

Answer: 1

Explanation:

There is no standard metric in CloudWatch for collecting EC2 memory usage. However, you can use the CloudWatch agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers. The metrics can be pushed to a CloudWatch custom metric.

CORRECT: "Install the CloudWatch agent on the EC2 instance to push memory usage to an Amazon CloudWatch custom metric" is the correct answer.

INCORRECT: "Use an instance type that supports memory usage reporting to a metric by default" is incorrect. There is no such thing as an EC2 instance type that supports memory usage reporting to a metric by default. The limitation is not in EC2 but in the metrics that are collected by CloudWatch.

INCORRECT: "Call Amazon CloudWatch to retrieve the memory usage metric data that exists for the EC2 instance" is incorrect. As there is no standard metric for collecting EC2 memory usage in CloudWatch the data will not already exist there to be retrieved.

INCORRECT: "Assign an IAM role to the EC2 instance with an IAM policy granting access to the desired metric" is incorrect. This is not an issue of permissions.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/>

QUESTION 55

An organization is migrating data to the AWS cloud. An on-premises application uses Network File System shares and must access the data without code changes. The data is critical and is accessed frequently.

Which storage solution should a Solutions Architect recommend to maximize availability and durability?

1. Amazon Elastic Block Store
2. Amazon Simple Storage Service
3. AWS Storage Gateway – File Gateway
4. Amazon Elastic File System

Answer: 3

Explanation:

The solution must use NFS file shares to access the migrated data without code modification. This means you can use either Amazon EFS or AWS Storage Gateway – File Gateway. Both of these can be mounted using NFS from on-premises applications.

However, EFS is the wrong answer as the solution asks to maximize availability and durability. The File Gateway backs off of Amazon S3 which has much higher availability and durability than EFS which is why it is the best solution for this scenario.

CORRECT: "AWS Storage Gateway – File Gateway" is the correct answer.

INCORRECT: "Amazon Elastic Block Store" is incorrect. Amazon EBS is not a suitable solution as it is a block-based (not file-based like NFS) storage solution that you mount to EC2 instances in the cloud – not from on-premises applications.

INCORRECT: "Amazon Simple Storage Service" is incorrect. Amazon S3 does not offer an NFS interface.

INCORRECT: "Amazon Elastic File System" is incorrect as explained above.

References:

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

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 56

A Solutions Architect needs to design a solution that will allow Website Developers to deploy static web content without managing server infrastructure. All web content must be accessed over HTTPS with a custom domain name. The solution should be scalable as the company continues to grow.

Which of the following will provide the MOST cost-effective solution?

1. Amazon S3 with a static website
2. Amazon CloudFront with an Amazon S3 bucket origin
3. AWS Lambda function with Amazon API Gateway
4. Amazon EC2 instance with Amazon EBS

Answer: 2

Explanation:

You can create an Amazon CloudFront distribution that uses an S3 bucket as the origin. This will allow you to serve the static content using the HTTPS protocol.

To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:

- Using a REST API endpoint as the origin with access restricted by an [origin access identity \(OAI\)](#).
- Using a website endpoint as the origin with anonymous (public) access allowed.
- Using a website endpoint as the origin with access restricted by a Referer header.

CORRECT: "Amazon CloudFront with an Amazon S3 bucket origin" is the correct answer.

INCORRECT: "Amazon S3 with a static website" is incorrect. You can create a static website using Amazon S3 with a custom domain name. However, you cannot connect to an Amazon S3 static website using HTTPS (only HTTP) so this solution does not work.

INCORRECT: "AWS Lambda function with Amazon API Gateway" is incorrect. AWS Lambda and API Gateway are both serverless services however this combination does not provide a solution for serving static content over HTTPS.

INCORRECT: "Amazon EC2 instance with Amazon EBS" is incorrect. Amazon EC2 with EBS is not a suitable solution as you would need to manage the server infrastructure (which the question states is not desired).

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 57

A Solutions Architect must design a storage solution for incoming billing reports in CSV format. The data will be analyzed infrequently and discarded after 30 days.

Which combination of services will be MOST cost-effective in meeting these requirements?

1. Write the files to an S3 bucket and use Amazon Athena to query the data
2. Import the logs to an Amazon Redshift cluster
3. Use AWS Data Pipeline to import the logs into a DynamoDB table
4. Import the logs into an RDS MySQL instance

Answer: 1

Explanation:

Amazon S3 is great solution for storing objects such as this. You only pay for what you use and don't need to worry about scaling as it will scale as much as you need it to. Using Amazon Athena to analyze the data works well as it is a serverless service so it will be very cost-effective for use cases where the analysis is only happening infrequently. You can also configure Amazon S3 to expire the objects after 30 days.

CORRECT: "Write the files to an S3 bucket and use Amazon Athena to query the data" is the correct answer.

INCORRECT: "Import the logs to an Amazon Redshift cluster" is incorrect. Importing the log files into an Amazon RedShift cluster will mean you can perform analytics on the data as this is the primary use case for RedShift (it's a data warehouse). However, this is not the most cost-effective solution as RedShift uses EC2 instances (it's not serverless) so the instances will be running all the time even though the analytics is infrequent.

INCORRECT: "Use AWS Data Pipeline to import the logs into a DynamoDB table" is incorrect. AWS Data Pipeline is used to process and move data. You can move data into DynamoDB, but this is not a good storage solution for these log files. Also, there is no analytics solution in this option.

INCORRECT: "Import the logs into an RDS MySQL instance" is incorrect. Importing the logs into an RDS MySQL instance is not a good solution. This is not the best storage solution for log files and its main use case as a DB is transactional rather than analytical.

References:

<https://aws.amazon.com/athena/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-athena/>

QUESTION 58

A Solutions Architect must design a solution that encrypts data in Amazon S3. Corporate policy mandates encryption keys be generated and managed on premises. Which solution should the Architect use to meet the security requirements?

1. SSE-C: Server-side encryption with customer-provided encryption keys
2. SSE-S3: Server-side encryption with Amazon-managed master key
3. SSE-KMS: Server-side encryption with AWS KMS managed keys
4. AWS CloudHSM

Answer: 1

Explanation:

Server-side encryption is about protecting data at rest. Server-side encryption encrypts only the object data, not object metadata. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages the encryption as it writes to disks and decryption when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.

When you upload an object, Amazon S3 uses the encryption key you provide to apply AES-256 encryption to your data and removes the encryption key from memory. When you retrieve an object, you must provide the same encryption key as part of your request. Amazon S3 first verifies that the encryption key you provided matches and then decrypts the object before returning the object data to you.

CORRECT: "SSE-C: Server-side encryption with customer-provided encryption keys" is the correct answer.

INCORRECT: "SSE-S3: Server-side encryption with Amazon-managed master key" is incorrect. With SSE-S3, Amazon manage the keys for you, so this is incorrect.

INCORRECT: "SSE-KMS: Server-side encryption with AWS KMS managed keys" is incorrect. With SSE-KMS the keys are managed in the Amazon Key Management Service, so this is incorrect.

INCORRECT: "AWS CloudHSM" is incorrect. With AWS CloudHSM your keys are held in AWS in a hardware security module. Again, the keys are not on-premises they are in AWS, so this is incorrect.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryptionCustomerKeys.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 59

A Solutions Architect must select the most appropriate database service for two use cases. A team of data scientists perform complex queries on a data warehouse that take several hours to complete. Another team of scientists need to run fast, repeat queries and update dashboards for customer support staff.

Which solution delivers these requirements MOST cost-effectively?

1. RedShift for both use cases
2. RDS for both use cases
3. RedShift for the analytics use case and ElastiCache in front of RedShift for the customer support dashboard
4. RedShift for the analytics use case and RDS for the customer support dashboard

Answer: 1

Explanation:

RedShift is a columnar data warehouse DB that is ideal for running long complex queries. RedShift can also improve performance for repeat queries by caching the result and returning the cached result when queries are re-run. Dashboard, visualization, and business intelligence (BI) tools that execute repeat queries see a significant boost in performance due to result caching.

CORRECT: "RedShift for both use cases" is the correct answer.

INCORRECT: "RDS for both use cases" is incorrect. RDS may be a good fit for the fast queries (not for the complex queries) but you now have multiple DBs to manage and multiple sets of data which is not going to be cost-effective.

INCORRECT: "RedShift for the analytics use case and ElastiCache in front of RedShift for the customer support dashboard" is incorrect. You could put ElastiCache in front of the RedShift DB and this would provide good performance for the fast, repeat queries. However, it is not essential and would add cost to the solution so is not the most cost-effective option available.

INCORRECT: "RedShift for the analytics use case and RDS for the customer support dashboard" is incorrect as RedShift is a better fit for both use cases.

References:

<https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-redshift-introduces-result-caching-for-sub-second-response-for-repeat-queries/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>

QUESTION 60

A DynamoDB database you manage is randomly experiencing heavy read requests that are causing latency. What is the simplest way to alleviate the performance issues?

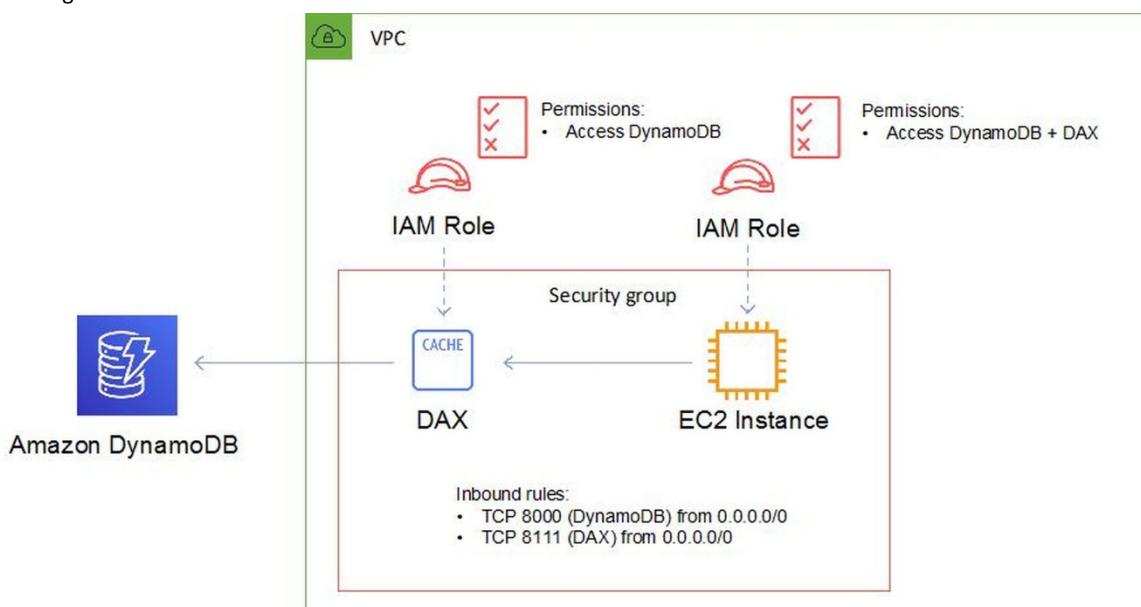
1. Create DynamoDB read replicas
2. Enable EC2 Auto Scaling for DynamoDB
3. Create an ElastiCache cluster in front of DynamoDB
4. Enable DynamoDB DAX

Answer: 4

Explanation:

DynamoDB offers consistent single-digit millisecond latency. However, DynamoDB + DAX further increases performance with response times in microseconds for millions of requests per second for read-heavy workloads.

The DAX cache uses cluster nodes running on Amazon EC2 instances and sits in front of the DynamoDB table as you can see in the diagram below:



CORRECT: "Enable DynamoDB DAX" is the correct answer.

INCORRECT: "Create DynamoDB read replicas" is incorrect. There's no such thing as DynamoDB Read Replicas (Read Replicas are an RDS concept).

INCORRECT: "Enable EC2 Auto Scaling for DynamoDB" is incorrect. You cannot use EC2 Auto Scaling with DynamoDB. You can use Application Auto Scaling to scale DynamoDB but as the spikes in read traffic are random and Auto Scaling needs time to adjust the capacity of the DB it wouldn't be as responsive as using DynamoDB DAX.

INCORRECT: "Create an ElastiCache cluster in front of DynamoDB" is incorrect. ElastiCache in front of DynamoDB is not the best answer as DynamoDB DAX is a simpler implementation and provides the required performance improvements.

References:

<https://aws.amazon.com/dynamodb/dax/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

QUESTION 61

A large media site has multiple applications running on Amazon ECS. A Solutions Architect needs to use content metadata to route traffic to specific services.

What is the MOST efficient method to fulfil this requirement?

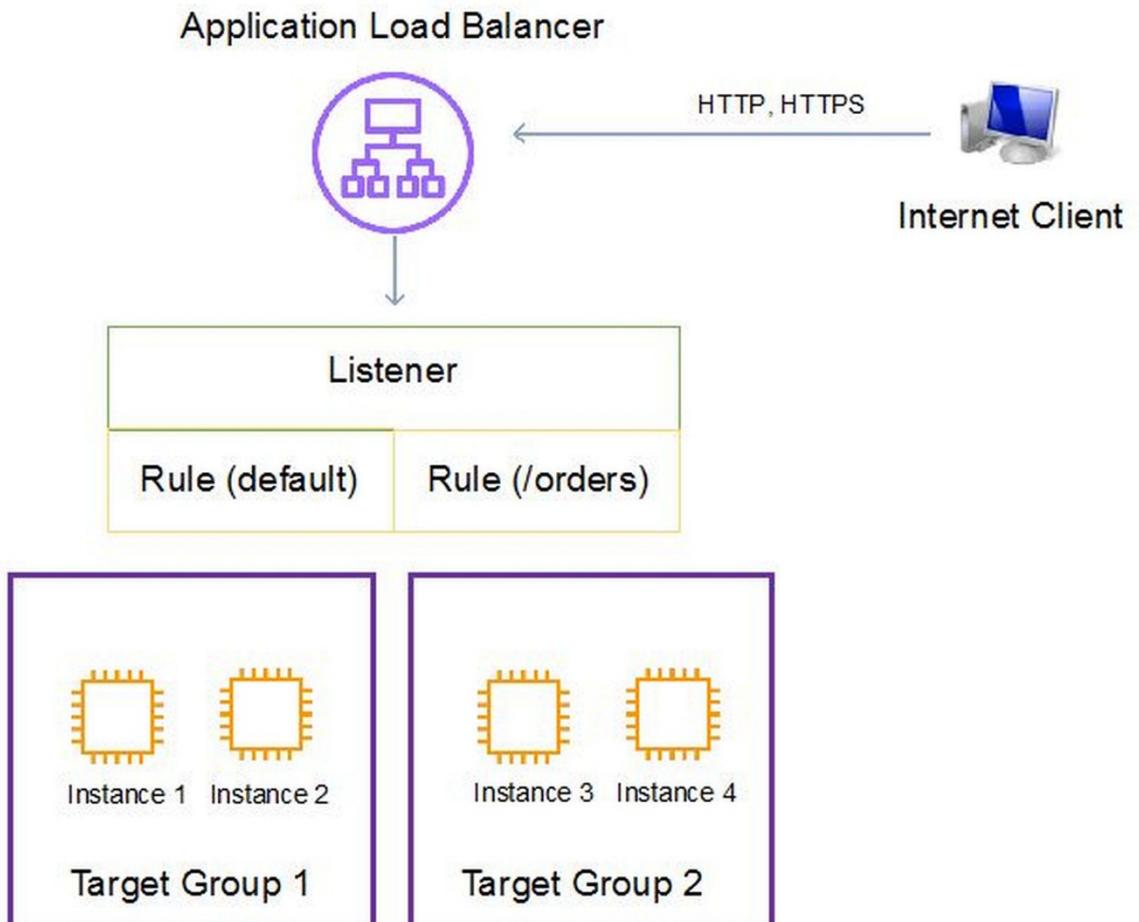
1. Use an AWS Classic Load Balancer with a host-based routing rule to route traffic to the correct service
2. Use the AWS CLI to update an Amazon Route 53 hosted zone to route traffic as services get updated
3. Use an AWS Application Load Balancer with a path-based routing rule to route traffic to the correct service
4. Use Amazon CloudFront to manage and route traffic to the correct service

Answer: 3

Explanation:

The ELB Application Load Balancer can route traffic based on data included in the request including the host name portion of the URL as well as the path in the URL. Creating a rule to route traffic based on information in the path will work for this solution and ALB works well with Amazon ECS.

The diagram below depicts a configuration where a listener directs traffic that comes in with /orders in the URL to the second target group and all other traffic to the first target group:



CORRECT: "Use an AWS Application Load Balancer with a path-based routing rule to route traffic to the correct service" is the correct answer.

INCORRECT: "Use an AWS Classic Load Balancer with a host-based routing rule to route traffic to the correct service" is incorrect. The ELB Classic Load Balancer does not support any content-based routing including host or path-based.

INCORRECT: "Use the AWS CLI to update an Amazon Route 53 hosted zone to route traffic as services get updated" is incorrect. Using the AWS CLI to update Route 53 as to how to route traffic may work, but it is definitely not the most efficient way to solve this challenge.

INCORRECT: "Use Amazon CloudFront to manage and route traffic to the correct service" is incorrect. Amazon CloudFront does not have the capability to route traffic to different Amazon ECS services based on content metadata.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 62

You have created a file system using Amazon Elastic File System (EFS) which will hold home directories for users. What else needs to be done to enable users to save files to the EFS file system?

1. Create a separate EFS file system for each user and grant read-write-execute permissions on the root directory to the respective user. Then mount the file system to the users' home directory

2. Modify permissions on the root directory to grant read-write-execute permissions to the users. Then create a subdirectory and mount it to the users' home directory
3. Instruct the users to create a subdirectory on the file system and mount the subdirectory to their home directory
4. Create a subdirectory for each user and grant read-write-execute permissions to the users. Then mount the subdirectory to the users' home directory

Answer: 4

Explanation:

After creating a file system, by default, only the root user (UID 0) has read-write-execute permissions. For other users to modify the file system, the root user must explicitly grant them access.

One common use case is to create a "writable" subdirectory under this file system root for each user you create on the EC2 instance and mount it on the user's home directory. All files and subdirectories the user creates in their home directory are then created on the Amazon EFS file system

CORRECT: "Create a subdirectory for each user and grant read-write-execute permissions to the users. Then mount the subdirectory to the users' home directory" is the correct answer.

INCORRECT: "Create a separate EFS file system for each user and grant read-write-execute permissions on the root directory to the respective user. Then mount the file system to the users' home directory" is incorrect. You don't want to create a separate EFS file system for each user, this would be a higher cost and require more management overhead.

INCORRECT: "Modify permissions on the root directory to grant read-write-execute permissions to the users. Then create a subdirectory and mount it to the users' home directory" is incorrect. You don't want to modify permission on the root directory as this will mean all users are able to access other users' files (and this is a home directory, so the contents are typically kept private).

INCORRECT: "Instruct the users to create a subdirectory on the file system and mount the subdirectory to their home directory" is incorrect. Instructing the users to create a subdirectory on the file system themselves would not work as they will not have access to write to the directory root.

References:

<https://docs.aws.amazon.com/efs/latest/ug/accessing-fs-nfs-permissions-per-user-subdirs.html>

<https://docs.aws.amazon.com/efs/latest/ug/accessing-fs-nfs-permissions.html#accessing-fs-nfs-permissions-ex-scenarios>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 63

An AWS workload in a VPC is running a legacy database on an Amazon EC2 instance. Data is stored on a 2000GB Amazon EBS (gp2) volume. At peak load times, logs show excessive wait time.

What should be implemented to improve database performance using persistent storage?

1. Change the EC2 instance type to one with burstable performance
2. Change the EC2 instance type to one with EC2 instance store volumes
3. Migrate the data on the Amazon EBS volume to an SSD-backed volume
4. Migrate the data on the EBS volume to provisioned IOPS SSD (io1)

Answer: 4

Explanation:

The data is already on an SSD-backed volume (gp2), therefore to improve performance the best option is to migrate the data onto a provisioned IOPS SSD (io1) volume type which will provide improved I/O performance and therefore reduce wait times.

CORRECT: "Migrate the data on the EBS volume to provisioned IOPS SSD (io1)" is the correct answer.

INCORRECT: "Change the EC2 instance type to one with burstable performance" is incorrect. Burstable performance instances provide a baseline of CPU performance with the ability to burst to a higher level when required. However, the issue in this scenario is disk wait time, not CPU performance, therefore we need to improve I/O not CPU performance.

INCORRECT: "Change the EC2 instance type to one with EC2 instance store volumes" is incorrect. Using an instance store volume may provide high performance but the data is not persistent so it is not suitable for a database.

INCORRECT: "Migrate the data on the Amazon EBS volume to an SSD-backed volume" is incorrect as the data is already on an SSD-backed volume (gp2).

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 64

A data-processing application runs on an i3.large EC2 instance with a single 100 GB EBS gp2 volume. The application stores temporary data in a small database (less than 30 GB) located on the EBS root volume. The application is struggling to process the data fast enough, and a Solutions Architect has determined that the I/O speed of the temporary database is the bottleneck.

What is the MOST cost-efficient way to improve the database response times?

1. Put the temporary database on a new 50-GB EBS io1 volume with a 3000 IOPS allocation
2. Move the temporary database onto instance storage
3. Put the temporary database on a new 50-GB EBS gp2 volume
4. Enable EBS optimization on the instance and keep the temporary files on the existing volume

Answer: 2

Explanation:

EC2 Instance Stores are high-speed ephemeral storage that is physically attached to the EC2 instance. The i3.large instance type comes with a single 475GB NVMe SSD instance store so it would be a good way to lower cost and improve performance by using the attached instance store. As the files are temporary, it can be assumed that ephemeral storage (which means the data is lost when the instance is stopped) is sufficient.

CORRECT: "Move the temporary database onto instance storage" is the correct answer.

INCORRECT: "Put the temporary database on a new 50-GB EBS io1 volume with a 3000 IOPS allocation" is incorrect. Moving the DB to a new 50-GB EBS io1 volume with a 3000 IOPS allocation will improve performance but is more expensive so will not be the most cost-efficient solution.

INCORRECT: "Put the temporary database on a new 50-GB EBS gp2 volume" is incorrect. Moving the DB to a new 50-GB EBS gp2 volume will not result in a performance improvement as you get IOPS allocated per GB so a smaller volume will have lower performance.

INCORRECT: "Enable EBS optimization on the instance and keep the temporary files on the existing volume" is incorrect.

Enabling EBS optimization will not lower cost. Also, EBS Optimization is a network traffic optimization, it does not change the I/O performance of the volume.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 65

An application is hosted on the U.S west coast. Users there have no problems, but users on the east coast are experiencing performance issues. The users have reported slow response times with the search bar autocomplete and display of account listings.

How can you improve the performance for users on the east coast?

1. Host the static content in an Amazon S3 bucket and distribute it using CloudFront
2. Setup cross-region replication and use Route 53 geolocation routing
3. Create a DynamoDB Read Replica in the U.S east region
4. Create an ElastiCache database in the U.S east region

Answer: 4

Explanation:

ElastiCache can be deployed in the U.S east region to provide high-speed access to the content. ElastiCache Redis has a good use case for autocomplete (see links below).

CORRECT: "Create an ElastiCache database in the U.S east region" is the correct answer.

INCORRECT: "Host the static content in an Amazon S3 bucket and distribute it using CloudFront" is incorrect. This is not static content that can be hosted in an Amazon S3 bucket and distributed using CloudFront.

INCORRECT: "Setup cross-region replication and use Route 53 geolocation routing" is incorrect. Cross-region replication is an Amazon S3 concept and the dynamic data that is presented by this application is unlikely to be stored in an S3 bucket.

INCORRECT: "Create a DynamoDB Read Replica in the U.S east region" is incorrect. There's no such thing as a DynamoDB Read Replica (Read Replicas are an RDS concept).

References:

<https://aws.amazon.com/blogs/database/creating-a-simple-autocompletion-service-with-redis-part-one-of-two/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticsearch/>

SET 3: PRACTICE QUESTIONS ONLY

For training purposes, go directly to [Set 3: Practice Questions, Answers & Explanations](#)

QUESTION 1

A security officer requires that access to company financial reports is logged. The reports are stored in an Amazon S3 bucket. Additionally, any modifications to the log files must be detected.

Which actions should a solutions architect take?

1. Use S3 server access logging on the bucket that houses the reports with the read and write data events and the log file validation options enabled
2. 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
3. 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
4. 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

QUESTION 2

A company operates a production web application that uses an Amazon RDS MySQL database. The database has automated, non-encrypted daily backups. To increase the security of the data, it has been recommended that encryption should be enabled for backups. Unencrypted backups will be destroyed after the first encrypted backup has been completed.

What should be done to enable encryption for future backups?

1. Enable default encryption for the Amazon S3 bucket where backups are stored
2. Modify the backup section of the database configuration to toggle the Enable encryption check box
3. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot
4. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance

QUESTION 3

A company has deployed an API in a VPC behind an internal Network Load Balancer (NLB). An application that consumes the API as a client is deployed in a second account in private subnets.

Which architectural configurations will allow the API to be consumed without using the public Internet? (Select TWO.)

1. Configure a VPC peering connection between the two VPCs. Access the API using the private address
2. Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address
3. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address
4. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address
5. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address

QUESTION 4

An application runs on Amazon EC2 Linux instances. The application generates log files which are written using standard API calls. A storage solution is required that can be used to store the files indefinitely and must allow concurrent access to all files.

Which storage service meets these requirements and is the MOST cost-effective?

1. Amazon EBS
2. Amazon EFS
3. Amazon EC2 instance store
4. Amazon S3

QUESTION 5

A production application runs on an Amazon RDS MySQL DB instance. A solutions architect is building 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?

1. Create a cross-region Multi-AZ deployment and create a read replica in the second region
2. Create a Multi-AZ RDS Read Replica of the production RDS DB instance
3. Use Amazon Data Lifecycle Manager to automatically create and manage snapshots
4. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica

QUESTION 6

An online store uses an Amazon Aurora database. The database is deployed as a Multi-AZ deployment. Recently, metrics have shown that database read requests are high and causing performance issues which result in latency for write requests.

What should the solutions architect do to separate the read requests from the write requests?

1. Enable read through caching on the Amazon Aurora database
2. Update the application to read from the Aurora Replica
3. Create a read replica and modify the application to use the appropriate endpoint
4. Create a second Amazon Aurora database and link it to the primary database as a read replica

QUESTION 7

An application is deployed on multiple AWS regions and accessed from around the world. The application exposes static public IP addresses. Some users are experiencing poor performance when accessing the application over the Internet.

What should a solutions architect recommend to reduce internet latency?

1. Set up AWS Global Accelerator and add endpoints
2. Set up AWS Direct Connect locations in multiple Regions
3. Set up an Amazon CloudFront distribution to access an application
4. Set up an Amazon Route 53 geoproximity routing policy to route traffic

QUESTION 8

A new application will be launched on an Amazon EC2 instance with an Elastic Block Store (EBS) volume. A solutions architect needs to determine the most cost-effective storage option. The application will have infrequent usage, with peaks of traffic for a couple of hours in the morning and evening. Disk I/O is variable with peaks of up to 3,000 IOPS.

Which solution should the solutions architect recommend?

1. Amazon EBS Cold HDD (sc1)
2. Amazon EBS General Purpose SSD (gp2)
3. Amazon EBS Provisioned IOPS SSD (io1)
4. Amazon EBS Throughput Optimized HDD (st1)

QUESTION 9

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

1. Create an ACL to provide access to the services or actions
2. Create a security group to allow accounts and attach it to user groups
3. Create cross-account roles in each account to deny access to the services or actions
4. Create a service control policy in the root organizational unit to deny access to the services or actions

QUESTION 10

A company is planning to use Amazon S3 to store documents uploaded by its customers. 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?

1. Server-Side Encryption with keys stored in an S3 bucket
2. Server-Side Encryption with Customer-Provided Keys (SSE-C)
3. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
4. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

QUESTION 11

A company has some statistical data stored in an Amazon RDS database. The company wants to allow users to access this information using an API. A solutions architect must create a solution that allows sporadic access to the data, ranging from no requests to large bursts of traffic.

Which solution should the solutions architect suggest?

1. Set up an Amazon API Gateway and use Amazon ECS
2. Set up an Amazon API Gateway and use AWS Elastic Beanstalk
3. Set up an Amazon API Gateway and use AWS Lambda functions
4. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling

QUESTION 12

A company runs a financial application using an Amazon EC2 Auto Scaling group behind an Application Load Balancer (ALB). When running month-end reports on a specific day and time each month the application becomes unacceptably slow. Amazon CloudWatch metrics show the CPU utilization hitting 100%.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

1. Configure an Amazon CloudFront distribution in front of the ALB
2. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization
3. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule
4. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances

QUESTION 13

A solutions architect is designing a high performance computing (HPC) application using Amazon EC2 Linux instances. All EC2 instances need to communicate to each other with low latency and high throughput network performance.

Which EC2 solution BEST meets these requirements?

1. Launch the EC2 instances in a cluster placement group in one Availability Zone
2. Launch the EC2 instances in a spread placement group in one Availability Zone
3. Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances
4. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

QUESTION 14

A web application in a three-tier architecture runs on a fleet of Amazon EC2 instances. Performance issues have been reported and investigations point to insufficient swap space. The operations team requires monitoring to determine if this is correct.

What should a solutions architect recommend?

1. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch
2. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch
3. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch

4. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch

QUESTION 15

A gaming company collects real-time data and stores it in an on-premises database system. The company are migrating to AWS and need better performance for the database. A solutions architect has been asked to recommend an in-memory database that supports data replication.

Which database should a solutions architect recommend?

1. Amazon RDS for MySQL
2. Amazon RDS for PostgreSQL
3. Amazon ElastiCache for Redis
4. Amazon ElastiCache for Memcached

QUESTION 16

A company has experienced malicious traffic from some suspicious IP addresses. The security team discovered the requests are from different IP addresses under the same CIDR range.

What should a solutions architect recommend to the team?

1. Add a rule in the inbound table of the security group to deny the traffic from that CIDR range
2. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range
3. Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules
4. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules

QUESTION 17

A solutions architect is designing a microservices architecture. AWS Lambda will store data in an Amazon DynamoDB table named Orders. The solutions architect needs to apply an IAM policy to the Lambda function's execution role to allow it to put, update, and delete items in the Orders table. No other actions should be allowed.

Which of the following code snippets should be included in the IAM policy to fulfill this requirement whilst providing the LEAST privileged access?

1.

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Allow",
>Action": [
    "dynamodb:PutItem",
    "dynamodb:UpdateItem",
    "dynamodb:DeleteItem"
],
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```
2.

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Allow",
>Action": [
    "dynamodb:PutItem",
    "dynamodb:UpdateItem",
    "dynamodb:DeleteItem"
],
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/*"
```

3.

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Allow",
>Action": "dynamodb:*",
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```

4.

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Deny",
>Action": "dynamodb:*",
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```

QUESTION 18

A company has created a duplicate of its environment in another AWS Region. The application is running in warm standby mode. There is an Application Load Balancer (ALB) in front of the application. Currently, failover is manual and requires updating a DNS alias record to point to the secondary ALB.

How can a solutions architect automate the failover process?

1. Enable an ALB health check
2. Enable an Amazon Route 53 health check
3. Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint
4. Create a latency based routing policy on Amazon Route 53

QUESTION 19

An application allows users to upload and download files. Files older than 2 years will be accessed less frequently. A solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend?

1. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard Infrequent Access (S3 Standard-IA)
2. Store the files on Amazon Elastic File System (EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA)
3. Store the files in Amazon Elastic Block Store (EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years
4. Store the files in Amazon Elastic Block Store (EBS) volumes. Create a lifecycle policy to move files older than 2 years to Amazon S3 Glacier

QUESTION 20

A company is planning to migrate a large quantity of important data to Amazon S3. The data will be uploaded to a versioning enabled bucket in the us-west-1 Region. The solution needs to include replication of the data to another Region for disaster recovery purposes.

How should a solutions architect configure the replication?

1. Create an additional S3 bucket in another Region and configure cross-Region replication
2. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)
3. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication
4. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)

QUESTION 21

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?

1. Use a simple scaling policy to dynamically scale the Auto Scaling group
2. Use a target tracking policy to dynamically scale the Auto Scaling group
3. Use an AWS Lambda function to update the desired Auto Scaling group capacity
4. Use scheduled scaling actions to scale up and scale down the Auto Scaling group

QUESTION 22

A High Performance Computing (HPC) application needs storage that can provide 135,000 IOPS. The storage layer is replicated across all instances in a cluster.

What is the optimal storage solution that provides the required performance and is cost-effective?

1. Use Amazon EBS Provisioned IOPS volume with 135,000 IOPS
2. Use Amazon Instance Store
3. Use Amazon S3 with byte-range fetch
4. Use Amazon EC2 Enhanced Networking with an EBS HDD Throughput Optimized volume

QUESTION 23

A high-performance file system is required for a financial modelling application. The data set will be stored on Amazon S3 and the storage solution must have seamless integration so objects can be accessed as files.

Which storage solution should be used?

1. Amazon FSx for Windows File Server
2. Amazon FSx for Lustre
3. Amazon Elastic File System (EFS)
4. Amazon Elastic Block Store (EBS)

QUESTION 24

An application requires a MySQL database which will only be used several times a week for short periods. The database needs to provide automatic instantiation and scaling. Which database service is most suitable?

1. Amazon RDS MySQL
2. Amazon EC2 instance with MySQL database installed
3. Amazon Aurora
4. Amazon Aurora Serverless

QUESTION 25

An Architect needs to find a way to automatically and repeatably create many member accounts within an AWS Organization. The accounts also need to be moved into an OU and have VPCs and subnets created.

What is the best way to achieve this?

1. Use the AWS Organizations API
2. Use CloudFormation with scripts
3. Use the AWS Management Console
4. Use the AWS CLI

QUESTION 26

An organization is extending a secure development environment into AWS. They have already secured the VPC including removing the Internet Gateway and setting up a Direct Connect connection. What else needs to be done to add encryption?

1. Setup a Virtual Private Gateway (VPG)
2. Enable IPsec encryption on the Direct Connect connection
3. Setup the Border Gateway Protocol (BGP) with encryption
4. Configure an AWS Direct Connect Gateway

QUESTION 27

A shared services VPC is being setup for use by several AWS accounts. An application needs to be securely shared from the shared services VPC. The solution should not allow consumers to connect to other instances in the VPC.

How can this be setup with the least administrative effort? (Select TWO.)

1. Create a Network Load Balancer (NLB)
2. Use AWS PrivateLink to expose the application as an endpoint service
3. Use AWS ClassicLink to expose the application as an endpoint service
4. Setup VPC peering between each AWS VPC
5. Configure security groups to restrict access

QUESTION 28

A web app allows users to upload images for viewing online. The compute layer that processes the images is behind an Auto Scaling group. The processing layer should be decoupled from the front end and the ASG needs to dynamically adjust based on the number of images being uploaded.

How can this be achieved?

1. Create an Amazon SNS Topic to generate a notification each time a message is uploaded. Have the ASG scale based on the number of SNS messages
2. Create a target tracking policy that keeps the ASG at 70% CPU utilization
3. Create an Amazon SQS queue and custom CloudWatch metric to measure the number of messages in the queue. Configure the ASG to scale based on the number of messages in the queue
4. Create a scheduled policy that scales the ASG at times of expected peak load

QUESTION 29

A web application is running on a fleet of Amazon EC2 instances using an Auto Scaling Group. It is desired that the CPU usage in the fleet is kept at 40%.

How should scaling be configured?

1. Use a simple scaling policy that launches instances when the average CPU hits 40%
2. Use a target tracking policy that keeps the average aggregate CPU utilization at 40%
3. Use a step scaling policy that uses the PercentChangeInCapacity value to adjust the group size as required
4. Use a custom CloudWatch alarm to monitor CPU usage and notify the ASG using Amazon SNS

QUESTION 30

Health related data in Amazon S3 needs to be frequently accessed for up to 90 days. After that time the data must be retained for compliance reasons for seven years and is rarely accessed.

Which storage classes should be used?

1. Store data in STANDARD for 90 days then transition the data to DEEP_ARCHIVE
2. Store data in INTELLIGENT_TIERING for 90 days then transition to STANDARD_IA
3. Store data in STANDARD for 90 days then expire the data
4. Store data in STANDARD for 90 days then transition to REDUCED_REDUNDANCY

QUESTION 31

An e-commerce web application needs a highly scalable key-value database. Which AWS database service should be used?

1. Amazon RDS
2. Amazon RedShift
3. Amazon DynamoDB
4. Amazon ElastiCache

QUESTION 32

A Solutions Architect is designing a mobile application that will capture receipt images to track expenses. The Architect wants to store the images on Amazon S3. However, uploading the images through the web server will create too much traffic.

What is the MOST efficient method to store images from a mobile application on Amazon S3?

1. Expand the web server fleet with Spot instances to provide the resources to handle the images
2. Upload to a second bucket, and have a Lambda event copy the image to the primary bucket
3. Upload to a separate Auto Scaling Group of server behind an ELB Classic Load Balancer, and have the server instances write to the Amazon S3 bucket
4. Upload directly to S3 using a pre-signed URL

QUESTION 33

A Kinesis consumer application is reading at a slower rate than expected. It has been identified that multiple consumer applications have total reads exceeding the per-shard limits. How can this situation be resolved?

1. Increase the number of shards in the Kinesis data stream
2. Implement API throttling to restrict the number of requests per-shard
3. Increase the number of read transactions per shard
4. Implement read throttling for the Kinesis data stream

QUESTION 34

You need to scale read operations for your Amazon Aurora DB within a region. To increase availability you also need to be able to failover if the primary instance fails.

What should you implement?

1. Aurora Replicas
2. A DB cluster
3. An Aurora Cluster Volume
4. Aurora Global Database

QUESTION 35

A Solutions Architect needs to monitor application logs and receive a notification whenever a specific number of occurrences of certain HTTP status code errors occur. Which tool should the Architect use?

1. CloudWatch Metrics
2. CloudWatch Events
3. CloudTrail Trails
4. CloudWatch Logs

QUESTION 36

An application consists of a web tier in a public subnet and a MySQL cluster hosted on Amazon EC2 instances in a private subnet. The MySQL instances must retrieve product data from a third-party provider over the internet. A Solutions Architect must determine a strategy to enable this access with maximum security and minimum operational overhead.

What should the Solutions Architect do to meet these requirements?

1. Deploy a NAT instance in the private subnet. Direct all internet traffic to the NAT instance.
2. Create an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the internet gateway.
3. Deploy a NAT gateway in the public subnet. Modify the route table in the private subnet to direct all internet traffic to the NAT gateway.
4. Create a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the virtual private gateway.

QUESTION 37

A company needs to migrate a large quantity of data from an on-premises environment to Amazon S3. The company is connected via an AWS Direct Connect (DX) connection. The company requires a fully managed solution that will keep the data private and automate and accelerate the replication of the data to AWS storage services.

Which solution should a Solutions Architect recommend?

1. Deploy an AWS Storage Gateway volume gateway in stored volume mode and take point-in-time copies of the volumes using AWS Backup.
2. Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a VPC endpoint.
3. Deploy an AWS Storage Gateway file gateway with a local cache and store the primary data set in Amazon S3.
4. Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a public endpoint.

QUESTION 38

A company has a Production VPC and a Pre-Production VPC. The Production VPC uses VPNs through a customer gateway to connect to a single device in an on-premises data center. The Pre-Production VPC uses a virtual private gateway attached to two AWS Direct Connect (DX) connections. Both VPCs are connected using a single VPC peering connection.

How can a Solutions Architect improve this architecture to remove any single point of failure?

1. Add an additional VPC peering connection between the two VPCs.
2. Add additional VPNs to the Production VPC from a second customer gateway device.
3. Add a set of VPNs between the Production and Pre-Production VPCs.
4. Add a second virtual private gateway and attach it to the Production VPC.

QUESTION 39

A Solutions Architect must design a solution to allow many Amazon EC2 instances across multiple subnets to access a shared data store. The data must be accessed by all instances simultaneously and access should use the NFS protocol. The solution must also be highly scalable and easy to implement.

Which solution best meets these requirements?

1. Configure an additional EC2 instance as a file server. Create a role in AWS IAM that grants permissions to the file share and attach the role to the EC2 instances.
2. Create an Amazon S3 bucket and configure a Network ACL. Grant the EC2 instances permission to access the bucket using the NFS protocol.
3. Create an Amazon EBS volume and create a resource-based policy that grants an AWS IAM role access to the data. Attach the role to the EC2 instances.
4. Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.

QUESTION 40

A company requires a fully managed replacement for an on-premises storage service. The company's employees often work remotely from various locations. The solution should also be easily accessible to systems connected to the on-premises environment.

Which solution meets these requirements?

1. Use AWS Transfer Acceleration to replicate files to Amazon S3 and enable public access.
2. Use Amazon FSx to create an SMB file share. Connect remote clients to the file share over a client VPN.
3. Use AWS DataSync to synchronize data between the on-premises service and Amazon S3.
4. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.

QUESTION 41

A company hosts statistical data in an Amazon S3 bucket that users around the world download from their website using a URL that resolves to a domain name. The company needs to provide low latency access to users and plans to use Amazon Route 53 for hosting DNS records.

Which solution meets these requirements?

1. Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.

2. Create an A record in Route 53, use 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.
3. Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. 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.
4. Create an A record in Route 53, use 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.

QUESTION 42

A company requires a high-performance file system that can be mounted on Amazon EC2 Windows instances and Amazon EC2 Linux instances. Applications running on the EC2 instances perform separate processing of the same files and the solution must provide a file system that can be mounted by all instances simultaneously.

Which solution meets these requirements?

1. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances.
2. Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances.
3. Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances.
4. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket.

QUESTION 43

A company is deploying an application that produces data that must be processed in the order it is received. The company requires a solution for decoupling the event data from the processing layer. The solution must minimize operational overhead.

How can a Solutions Architect meet these requirements?

1. Create an Amazon SQS standard queue to decouple the application. Set up an AWS Lambda function to process messages from the queue independently.
2. Create an Amazon SNS topic to decouple the application. Configure an AWS Lambda function as a subscriber.
3. Create an Amazon SQS FIFO queue to decouple the application. Configure an AWS Lambda function to process messages from the queue.
4. Create an Amazon SNS topic to decouple the application. Configure an Amazon SQS queue as a subscriber.

QUESTION 44

An application runs on-premises and produces data that must be stored in a locally accessible file system that servers can mount using the NFS protocol. The data must be subsequently analyzed by Amazon EC2 instances in the AWS Cloud.

How can these requirements be met?

1. Use an AWS Storage Gateway tape gateway to take a backup of the local data and store it on AWS, then perform analytics on this data in the AWS Cloud.
2. Use an AWS Storage Gateway volume gateway in stored mode to regularly take snapshots of the local data, then copy the data to AWS.
3. Use an AWS Storage Gateway volume gateway in cached mode to back up all the local storage in the AWS Cloud, then perform analytics on this data in the cloud.
4. Use an AWS Storage Gateway file gateway to provide a locally accessible file system that replicates data to the cloud, then analyze the data in the AWS Cloud.

QUESTION 45

A company has created an application that stores sales performance data in an Amazon DynamoDB table. A web application is being created to display the data. A Solutions Architect must design the web application using managed services that require minimal operational maintenance.

Which architectures meet these requirements? (Select TWO.)

1. An Amazon API Gateway REST API directly accesses the sales performance data in the DynamoDB table.
2. An Elastic Load Balancer forwards requests to a target group with the DynamoDB table configured as the target.
3. An Amazon API Gateway REST API invokes an AWS Lambda function. The Lambda function reads data from the DynamoDB table.
4. An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that reads data from the DynamoDB table.
5. An Amazon Route 53 hosted zone routes requests to an AWS Lambda endpoint to invoke a Lambda function that reads data from the DynamoDB table.

QUESTION 46

A company runs a business-critical application in the us-east-1 Region. The application uses an Amazon Aurora MySQL database cluster which is 2 TB in size. A Solutions Architect needs to determine a disaster recovery strategy for failover to the us-west-2 Region. The strategy must provide a recovery time objective (RTO) of 10 minutes and a recovery point objective (RPO) of 5 minutes.

Which strategy will meet these requirements?

1. 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.
2. 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. Use an Amazon EventBridge rule that invokes an AWS Lambda function to promote the DB cluster in us-west-2 when failure is detected.
3. Create a cross-Region Aurora MySQL read replica in us-west-2 Region. Configure an Amazon EventBridge rule that invokes an AWS Lambda function that promotes the read replica in us-west-2 when failure is detected.
4. Recreate the database as an Aurora multi master cluster across the us-east-1 and us-west-2 Regions with multiple writers to allow read/write capabilities from all database instances.

QUESTION 47

An application runs on a fleet of Amazon EC2 instances in an Amazon EC2 Auto Scaling group behind an Elastic Load Balancer. The operations team has determined that the application performs best when the CPU utilization of the EC2 instances is at or near 60%.

Which scaling configuration should a Solutions Architect use to optimize the applications performance?

1. Use a simple scaling policy to dynamically scale the Auto Scaling group.
2. Use a step scaling policy to dynamically scale the Auto Scaling group.
3. Use a scheduled scaling policy to dynamically the Auto Scaling group.
4. Use a target tracking policy to dynamically scale the Auto Scaling group.

QUESTION 48

A company's staff connect from home office locations to administer applications using bastion hosts in a single AWS Region. The company requires a resilient bastion host architecture that requires minimal ongoing operational overhead.

How can a Solutions Architect best meet these requirements?

1. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones.
2. Create a Network Load Balancer backed by Reserved Instances in a cluster placement group.
3. Create a Network Load Balancer backed by the existing servers in different Availability Zones.
4. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple AWS Regions.

QUESTION 49

A Solutions Architect has been tasked with migrating 30 TB of data from an on-premises data center within 20 days. The company has an internet connection that is limited to 25 Mbps and the data transfer cannot use more than 50% of the connection speed.

What should a Solutions Architect do to meet these requirements?

1. Use AWS DataSync.

2. Use AWS Storage Gateway.
3. Use AWS Snowball.
4. Use a site-to-site VPN.

QUESTION 50

A company runs a containerized application on an Amazon Elastic Kubernetes Service (EKS) using a microservices architecture. The company requires a solution to collect, aggregate, and summarize metrics and logs. The solution should provide a centralized dashboard for viewing information including CPU and memory utilization for EKS namespaces, services, and pods.

Which solution meets these requirements?

1. Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
2. Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
3. Migrate the containers to Amazon ECS and enable Amazon CloudWatch Container Insights. View the metrics and logs in the CloudWatch console.
4. Configure AWS X-Ray to enable tracing for the EKS microservices. Query the trace data using Amazon Elasticsearch.

QUESTION 51

A company is deploying a solution for sharing media files around the world using Amazon CloudFront with an Amazon S3 origin configured as a static website. The company requires that all traffic for the website must be inspected by AWS WAF.

Which solution meets these requirements?

1. Deploy CloudFront with an S3 origin and configure an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the CloudFront distribution.
2. Create a Network ACL that limits access to the S3 bucket to the CloudFront IP addresses. Attach a WebACL to the CloudFront distribution.
3. Use an Amazon Route 53 Alias record to forward traffic for the website to AWS WAF. Configure AWS WAF to inspect traffic and attach the CloudFront distribution.
4. Create an S3 bucket policy with a condition that only allows requests that originate from AWS WAF.

QUESTION 52

A company has created a disaster recovery solution for an application that runs behind an Application Load Balancer (ALB). The DR solution consists of a second copy of the application running behind a second ALB in another Region. The Solutions Architect requires a method of automatically updating the DNS record to point to the ALB in the second Region.

What action should the Solutions Architect take?

1. Enable an ALB health check.
2. Use Amazon EventBridge to cluster the ALBs.
3. Enable an Amazon Route 53 health check.
4. Configure an alarm on a CloudTrail trail.

QUESTION 53

A company has deployed an application that consists of several microservices running on Amazon EC2 instances behind an Amazon API Gateway API. A Solutions Architect is concerned that the microservices are not designed to elastically scale when large increases in demand occur.

Which solution addresses this concern?

1. Create an Amazon SQS queue to store incoming requests. Configure the microservices to retrieve the requests from the queue for processing.
2. Use Amazon CloudWatch alarms to notify operations staff when the microservices are suffering high CPU utilization.
3. Spread the microservices across multiple Availability Zones and configure Amazon Data Lifecycle Manager to take regular snapshots.
4. Use an Elastic Load Balancer to distribute the traffic between the microservices. Configure Amazon CloudWatch metrics to monitor traffic to the microservices.

QUESTION 54

A Solutions Architect is designing a solution for an application that requires very low latency between the client and the backend. The application uses the UDP protocol, and the backend is hosted on Amazon EC2 instances. The solution must be highly available across multiple Regions and users around the world should be directed to the most appropriate Region based on performance.

How can the Solutions Architect meet these requirements?

1. Deploy Amazon EC2 instances in multiple Regions. Create a multivalue answer routing record in Amazon Route 53 that includes all EC2 endpoints.
2. Deploy an Application Load Balancer in front of the EC2 instances in each Region. Use AWS WAF to direct traffic to the most optimal Regional endpoint.
3. Deploy an Amazon CloudFront distribution with a custom origin pointing to Amazon EC2 instances in multiple Regions.
4. Deploy a Network Load Balancer in front of the EC2 instances in each Region. Use AWS Global Accelerator to route traffic to the most optimal Regional endpoint.

QUESTION 55

An application has multiple components for receiving requests that must be processed and subsequently processing the requests. The company requires a solution for decoupling the application components. The application receives around 10,000 requests per day and requests can take up to 2 days to process. Requests that fail to process must be retained.

Which solution meets these requirements most efficiently?

1. Create an Amazon DynamoDB table and enable DynamoDB streams. Configure the processing component to process requests from the stream.
2. Decouple the application components with an Amazon SQS queue. Configure a dead-letter queue to collect the requests that failed to process.
3. Use an Amazon Kinesis data stream to decouple application components and integrate the processing component with the Kinesis Client Library (KCL).
4. Decouple the application components with an Amazon SQS Topic. Configure the receiving component to subscribe to the SNS Topic.

QUESTION 56

A Solutions Architect created the following policy and associated to an AWS IAM group containing several administrative users:

{

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:TerminateInstances",
        "Resource": "*",
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": "10.1.2.0/24"
            }
        }
    },
    {
        "Effect": "Deny",
        "Action": "ec2:*",
        "Resource": "*",
    }
],
```

```

        "Condition": {
            "StringNotEquals": {
                "ec2:Region": "us-east-1"
            }
        }
    }
}

```

What is the effect of this policy?

1. Administrators can terminate an EC2 instance in any AWS Region except us-east-1.
2. Administrators can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28.
3. Administrators can terminate an EC2 instance with the IP address 10.1.2.5 in the us-east-1 Region.
4. Administrators cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28.

QUESTION 57

A company has several AWS accounts that are used by developers for development, testing and pre-production environments. The company has received large bills for Amazon EC2 instances that are underutilized. A Solutions Architect has been tasked with restricting the ability to launch large EC2 instances in all accounts.

How can the Solutions Architect meet this requirement with the LEAST operational overhead?

1. Create a service-linked role for Amazon EC2 and attach a policy that denies the launch of large EC2 instances.
2. Create a resource-based policy that denies the launch of large EC2 instances and attach it to Amazon EC2 in each account.
3. Create an organization in AWS Organizations that includes all accounts and create a service control policy (SCP) that denies the launch of large EC2 instances.
4. Create an IAM role in each account that denies the launch of large EC2 instances. Grant the developers IAM group access to the role.

QUESTION 58

A Solutions Architect is designing an application that will run on Amazon EC2 instances. The application will use Amazon S3 for storing image files and an Amazon DynamoDB table for storing customer information. The security team require that traffic between the EC2 instances and AWS services must not traverse the public internet.

How can the Solutions Architect meet the security team's requirements?

1. Create gateway VPC endpoints for Amazon S3 and DynamoDB.
2. Create a NAT gateway in a public subnet and configure route tables.
3. Create interface VPC endpoints for Amazon S3 and DynamoDB.
4. Create a virtual private gateway and configure VPC route tables.

QUESTION 59

A Solutions Architect needs a solution for hosting a website that will be used by a development team. The website contents will consist of HTML, CSS, client-side JavaScript, and images.

Which solution is MOST cost-effective?

1. Launch an Amazon EC2 instance and host the website there.
2. Use a Docker container to host the website on AWS Fargate.
3. Create an Application Load Balancer with an AWS Lambda target.
4. Create an Amazon S3 bucket and host the website there.

QUESTION 60

An application runs on Amazon EC2 instances in a private subnet. The EC2 instances process data that is stored in an Amazon S3 bucket. The data is highly confidential and a private and secure connection is required between the EC2 instances and the S3

bucket.

Which solution meets these requirements?

1. Configure encryption for the S3 bucket using an AWS KMS key.
2. Configure a custom SSL/TLS certificate on the S3 bucket.
3. Set up S3 bucket policies to allow access from a VPC endpoint.
4. Set up an IAM policy to grant read-write access to the S3 bucket.

QUESTION 61

A systems administrator of a company wants to detect and remediate the compromise of services such as Amazon EC2 instances and Amazon S3 buckets.

Which AWS service can the administrator use to protect the company against attacks?

1. Amazon Cognito
2. Amazon Inspector
3. Amazon Macie
4. Amazon GuardDuty

QUESTION 62

A company is creating a solution that must offer disaster recovery across multiple AWS Regions. The solution requires relational a database that can support a Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

1. Amazon RDS for with Multi-AZ enabled.
2. Amazon DynamoDB global tables.
3. Amazon Aurora Global Database.
4. Amazon RDS for with a cross-Region replica.

QUESTION 63

A company is deploying an analytics application on AWS Fargate. The application requires connected storage that offers concurrent access to files and high performance.

Which storage option should the solutions architect recommend?

1. Create an Amazon EFS file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
2. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
3. Create an Amazon EBS volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.
4. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.

QUESTION 64

An application runs on Amazon EC2 instances backed by Amazon EBS volumes and an Amazon RDS database. The application is highly sensitive and security compliance requirements mandate that all personally identifiable information (PII) be encrypted at rest.

Which solution should a Solutions Architect choose to this requirement?

1. Enable encryption on Amazon RDS during creation. Use Amazon Macie to identify sensitive data.
2. Configure Amazon EBS encryption and Amazon RDS encryption with AWS KMS keys to encrypt instance and database volumes.
3. Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes.
4. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.

QUESTION 65

An application generates unique files that are returned to customers after they submit requests to the application. The application uses an Amazon CloudFront distribution for sending the files to customers. The company wishes to reduce data transfer costs without modifying the application.

How can this be accomplished?

1. Enable caching on the CloudFront distribution to store generated files at the edge.
2. Use AWS Global Accelerator to reduce application latency for customers.
3. Enable Amazon S3 Transfer Acceleration to reduce the transfer times.
4. Use Lambda@Edge to compress the files as they are sent to users.

SET 3: PRACTICE QUESTIONS AND ANSWERS

QUESTION 1

A security officer requires that access to company financial reports is logged. The reports are stored in an Amazon S3 bucket. Additionally, any modifications to the log files must be detected.

Which actions should a solutions architect take?

1. Use S3 server access logging on the bucket that houses the reports with the read and write data events and the log file validation options enabled
2. 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
3. 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
4. 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: 3

Explanation:

Amazon CloudTrail can be used to log activity on the reports. The key difference between the two answers that include CloudTrail is that one references data events whereas the other references management events.

Data events provide visibility into the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities.

Example data events include:

- Amazon S3 object-level API activity (for example, GetObject, DeleteObject, and PutObject API operations).
- AWS Lambda function execution activity (the Invoke API).

Management events provide visibility into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Example management events include:

- Configuring security (for example, IAM AttachRolePolicy API operations)
- Registering devices (for example, Amazon EC2 CreateDefaultVpc API operations).

Therefore, to log data about access to the S3 objects the solutions architect should log read and write data events.

Data events

Data events are records of resource operations performed on or within a resource. These are also known as data plane operations. Additional charges apply. [Learn more](#)

S3 Lambda

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional charges apply. [Learn more](#)

Showing 1 of 1 resources				
Bucket name	Prefix	Read	Write	
<input type="checkbox"/> Select all S3 buckets in your account <small>?</small>		<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	
dctlabs	/ Prefix (optional)	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	

Log file validation can also be enabled on the destination bucket:

Storage location

Create a new S3 bucket Yes No

S3 bucket* 

Advanced

Log file prefix 
Location: /AWSLogs/515148227241/CloudTrail/ap-southeast-2

Encrypt log files with SSE-KMS Yes No 

Enable log file validation Yes No 

Send SNS notification for every log file delivery Yes No 

CORRECT: "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" is the correct answer.

INCORRECT: "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" is incorrect as data events should be logged rather than management events.

INCORRECT: "Use S3 server access logging on the bucket that houses the reports with the read and write data events and the log file validation options enabled" is incorrect as server access logging does not have an option for choosing data events or log file validation.

INCORRECT: "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" is incorrect as server access logging does not have an option for choosing management events or log file validation.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudtrail/>

QUESTION 2

A company operates a production web application that uses an Amazon RDS MySQL database. The database has automated, non-encrypted daily backups. To increase the security of the data, it has been recommended that encryption should be enabled for backups. Unencrypted backups will be destroyed after the first encrypted backup has been completed.

What should be done to enable encryption for future backups?

1. Enable default encryption for the Amazon S3 bucket where backups are stored
2. Modify the backup section of the database configuration to toggle the Enable encryption check box
3. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot
4. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance

Answer: 3

Explanation:

Amazon RDS uses snapshots for backup. Snapshots are encrypted when created only if the database is encrypted and you can

only select encryption for the database when you first create it. In this case the database, and hence the snapshots, are unencrypted.

However, you can create an encrypted copy of a snapshot. You can restore using that snapshot which creates a new DB instance that has encryption enabled. From that point on encryption will be enabled for all snapshots.

CORRECT: "Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot" is the correct answer.

INCORRECT: "Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance" is incorrect as you cannot create an encrypted read replica from an unencrypted master.

INCORRECT: "Modify the backup section of the database configuration to toggle the Enable encryption check box" is incorrect as you cannot add encryption for an existing database.

INCORRECT: "Enable default encryption for the Amazon S3 bucket where backups are stored" is incorrect because you do not have access to the S3 bucket in which snapshots are stored.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 3

A company has deployed an API in a VPC behind an internal Network Load Balancer (NLB). An application that consumes the API as a client is deployed in a second account in private subnets.

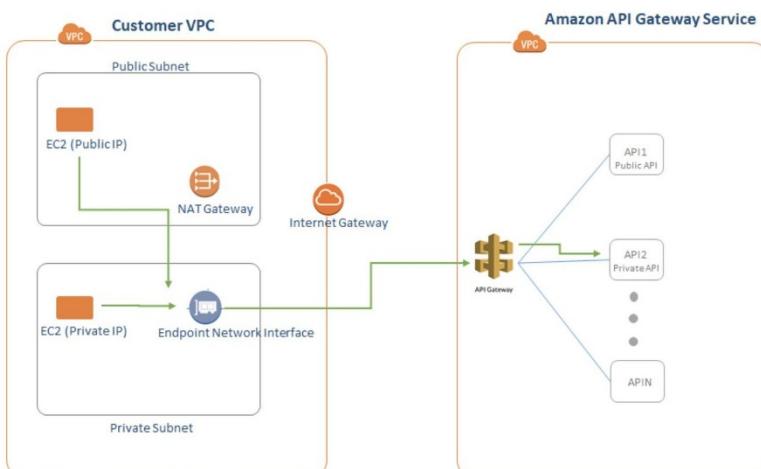
Which architectural configurations will allow the API to be consumed without using the public Internet? (Select TWO.)

1. Configure a VPC peering connection between the two VPCs. Access the API using the private address
2. Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address
3. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address
4. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address
5. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address

Answer: 1,4

Explanation:

You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an *endpoint service*). Other AWS principals can create a connection from their VPC to your endpoint service using an [interface VPC endpoint](#). You are the *service provider*, and the AWS principals that create connections to your service are *service consumers*.



This configuration is powered by AWS PrivateLink and clients do not need to use an internet gateway, NAT device, VPN connection or AWS Direct Connect connection, nor do they require public IP addresses.

Another option is to use a VPC Peering connection. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.

CORRECT: "Configure a VPC peering connection between the two VPCs. Access the API using the private address" is a correct answer.

CORRECT: "Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address" is also a correct answer.

INCORRECT: "Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address" is incorrect. Direct Connect is used for connecting from on-premises data centers into AWS. It is not used from one VPC to another.

INCORRECT: "Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address" is incorrect. ClassicLink allows you to link EC2-Classic instances to a VPC in your account, within the same Region. This is not relevant to sending data between two VPCs.

INCORRECT: "Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address" is incorrect. AWS RAM lets you share resources that are provisioned and managed in other AWS services. However, APIs are not shareable resources with AWS RAM.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service.html>

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 4

An application runs on Amazon EC2 Linux instances. The application generates log files which are written using standard API calls. A storage solution is required that can be used to store the files indefinitely and must allow concurrent access to all files.

Which storage service meets these requirements and is the MOST cost-effective?

1. Amazon EBS
2. Amazon EFS
3. Amazon EC2 instance store
4. Amazon S3

Answer: 4

Explanation:

The application is writing the files using API calls which means it will be compatible with Amazon S3 which uses a REST API. S3 is a massively scalable key-based object store that is well-suited to allowing concurrent access to the files from many instances.

Amazon S3 will also be the most cost-effective choice. A rough calculation using the AWS pricing calculator shows the cost differences between 1TB of storage on EBS, EFS, and S3 Standard.

Amazon Elastic Block Store (EBS) Region: US East (Ohio)	<button>Edit</button>	<button>Action ▾</button>
Amazon Elastic Block Storage (EBS) Number of instances (1), Average duration each instance runs (750 hours per month), Storage amount (1 TB), Snapshot Frequency (2x Daily), Amount changed per snapshot (3 GB)	Monthly:	158.09 USD
Amazon Elastic File System (EFS) Region: US East (Ohio)	<button>Edit</button>	<button>Action ▾</button>
Data stored in Standard storage (1 TB per month)	Monthly:	307.20 USD
Amazon Simple Storage Service (S3)	<button>Edit</button>	<button>Action ▾</button>
S3 Standard storage (1 TB per month)	Monthly:	24.45 USD

CORRECT: "Amazon S3" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as though this does offer concurrent access from many EC2 Linux instances, it is not the most cost-effective solution.

INCORRECT: "Amazon EBS" is incorrect. The Elastic Block Store (EBS) is not a good solution for concurrent access from many EC2 instances and is not the most cost-effective option either. EBS volumes are mounted to a single instance except when using multi-attach which is a new feature and has several constraints.

INCORRECT: "Amazon EC2 instance store" is incorrect as this is an ephemeral storage solution which means the data is lost when powered down. Therefore, this is not an option for long-term data storage.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 5

A production application runs on an Amazon RDS MySQL DB instance. A solutions architect is building 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?

1. Create a cross-region Multi-AZ deployment and create a read replica in the second region
2. Create a Multi-AZ RDS Read Replica of the production RDS DB instance
3. Use Amazon Data Lifecycle Manager to automatically create and manage snapshots
4. 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: 2

Explanation:

You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

CORRECT: "Create a Multi-AZ RDS Read Replica of the production RDS DB instance" is the correct answer.

INCORRECT: "Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica" is incorrect. Read replicas are primarily used for horizontal scaling. The best solution for high availability is to use a Multi-AZ read replica.

INCORRECT: "Create a cross-region Multi-AZ deployment and create a read replica in the second region" is incorrect as you cannot create a cross-region Multi-AZ deployment with RDS.

INCORRECT: "Use Amazon Data Lifecycle Manager to automatically create and manage snapshots" is incorrect as using snapshots is not the best solution for high availability.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html#USER_MySQL.Replication.ReadReplicas.MultiAZ

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 6

An online store uses an Amazon Aurora database. The database is deployed as a Multi-AZ deployment. Recently, metrics have shown that database read requests are high and causing performance issues which result in latency for write requests.

What should the solutions architect do to separate the read requests from the write requests?

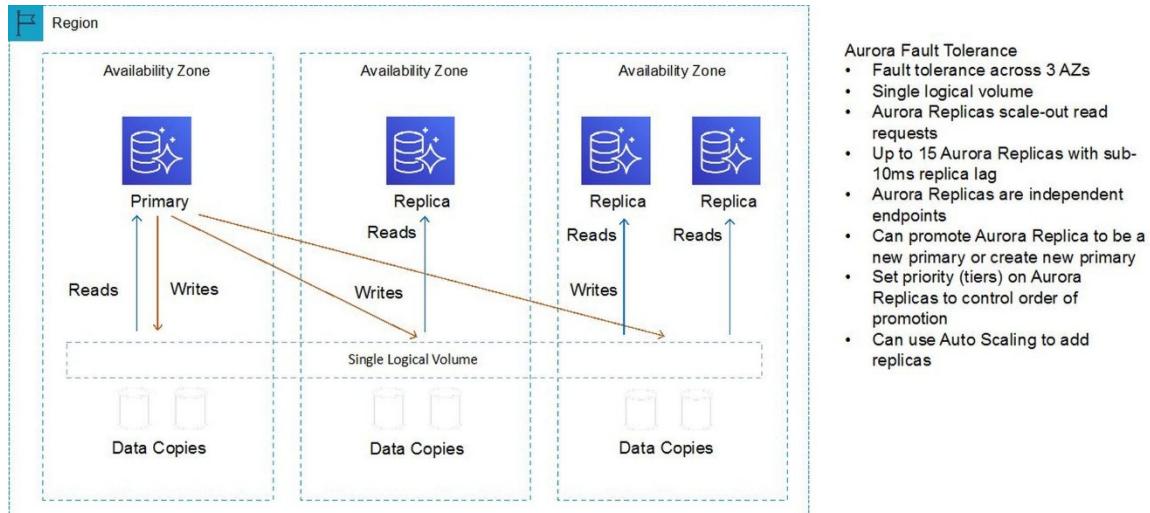
1. Enable read through caching on the Amazon Aurora database
2. Update the application to read from the Aurora Replica
3. Create a read replica and modify the application to use the appropriate endpoint
4. Create a second Amazon Aurora database and link it to the primary database as a read replica

Answer: 2

Explanation:

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region.

The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster.



As well as providing scaling for reads, Aurora Replicas are also targets for multi-AZ. In this case the solutions architect can update the application to read from the Aurora Replica.

CORRECT: "Update the application to read from the Aurora Replica" is the correct answer.

INCORRECT: "Create a read replica and modify the application to use the appropriate endpoint" is incorrect. An Aurora Replica is both a standby in a Multi-AZ configuration and a target for read traffic. The architect simply needs to direct traffic to the Aurora Replica.

INCORRECT: "Enable read through caching on the Amazon Aurora database." is incorrect as this is not a feature of Amazon Aurora.

INCORRECT: "Create a second Amazon Aurora database and link it to the primary database as a read replica" is incorrect as an

Aurora Replica already exists as this is a Multi-AZ configuration and the standby is an Aurora Replica that can be used for read traffic.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>

QUESTION 7

An application is deployed on multiple AWS regions and accessed from around the world. The application exposes static public IP addresses. Some users are experiencing poor performance when accessing the application over the Internet.

What should a solutions architect recommend to reduce internet latency?

1. Set up AWS Global Accelerator and add endpoints
2. Set up AWS Direct Connect locations in multiple Regions
3. Set up an Amazon CloudFront distribution to access an application
4. Set up an Amazon Route 53 geoproximity routing policy to route traffic

Answer: 1

Explanation:

AWS Global Accelerator is a service in which you create *accelerators* to improve availability and performance of your applications for local and global users. Global Accelerator directs traffic to optimal endpoints over the AWS global network. This improves the availability and performance of your internet applications that are used by a global audience. Global Accelerator is a global service that supports endpoints in multiple AWS Regions, which are listed in the [AWS Region Table](#).

By default, Global Accelerator provides you with two static IP addresses that you associate with your accelerator. (Or, instead of using the IP addresses that Global Accelerator provides, you can configure these entry points to be IPv4 addresses from your own IP address ranges that you bring to Global Accelerator.)



The static IP addresses are anycast from the AWS edge network and distribute incoming application traffic across multiple endpoint resources in multiple AWS Regions, which increases the availability of your applications. Endpoints can be Network Load Balancers, Application Load Balancers, EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.

CORRECT: "Set up AWS Global Accelerator and add endpoints" is the correct answer.

INCORRECT: "Set up AWS Direct Connect locations in multiple Regions" is incorrect as this is used to connect from an on-premises data center to AWS. It does not improve performance for users who are not connected to the on-premises data

center.

INCORRECT: "Set up an Amazon CloudFront distribution to access an application" is incorrect as CloudFront cannot expose static public IP addresses.

INCORRECT: "Set up an Amazon Route 53 geoproximity routing policy to route traffic" is incorrect as this does not reduce internet latency as well as using Global Accelerator. GA will direct users to the closest edge location and then use the AWS global network.

References:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-global-accelerator/>

QUESTION 8

A new application will be launched on an Amazon EC2 instance with an Elastic Block Store (EBS) volume. A solutions architect needs to determine the most cost-effective storage option. The application will have infrequent usage, with peaks of traffic for a couple of hours in the morning and evening. Disk I/O is variable with peaks of up to 3,000 IOPS.

Which solution should the solutions architect recommend?

1. Amazon EBS Cold HDD (sc1)
2. Amazon EBS General Purpose SSD (gp2)
3. Amazon EBS Provisioned IOPS SSD (io1)
4. Amazon EBS Throughput Optimized HDD (st1)

Answer: 2

Explanation:

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time.

Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

In this case the volume would have a baseline performance of $3 \times 200 = 600$ IOPS. The volume could also burst to 3,000 IOPS for extended periods. As the I/O varies, this should be suitable.

CORRECT: "Amazon EBS General Purpose SSD (gp2)" is the correct answer.

INCORRECT: "Amazon EBS Provisioned IOPS SSD (io1)" is incorrect as this would be a more expensive option and is not required for the performance characteristics of this workload.

INCORRECT: "Amazon EBS Cold HDD (sc1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.

INCORRECT: "Amazon EBS Throughput Optimized HDD (st1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 9

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

1. Create an ACL to provide access to the services or actions
2. Create a security group to allow accounts and attach it to user groups
3. Create cross-account roles in each account to deny access to the services or actions
4. Create a service control policy in the root organizational unit to deny access to the services or actions

Answer: 4

Explanation:

Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.



SCPs alone are not sufficient for allowing access in the accounts in your organization. Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a guardrail for what actions the principals can perform. You still need to attach [identity-based or resource-based policies](#) to principals or resources in your organization's accounts to actually grant permissions to them.

CORRECT: "Create a service control policy in the root organizational unit to deny access to the services or actions" is the correct answer.

INCORRECT: "Create an ACL to provide access to the services or actions" is incorrect as access control lists are not used for permissions associated with IAM. Permissions policies are used with IAM.

INCORRECT: "Create a security group to allow accounts and attach it to user groups" is incorrect as security groups are instance level firewalls. They do not limit service actions.

INCORRECT: "Create cross-account roles in each account to deny access to the services or actions" is incorrect as this is a complex solution and does not provide centralized control

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-organizations/>

QUESTION 10

A company is planning to use Amazon S3 to store documents uploaded by its customers. 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?

1. Server-Side Encryption with keys stored in an S3 bucket
2. Server-Side Encryption with Customer-Provided Keys (SSE-C)
3. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
4. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Answer: 4

Explanation:

SSE-KMS requires that AWS manage the data key but you manage the [customer master key](#) (CMK) in AWS KMS. You can choose

a [customer managed CMK](#) or the [AWS managed CMK](#) for Amazon S3 in your account.

Customer managed CMKs are CMKs in your AWS account that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their [key policies](#), [IAM policies](#), and [grants](#), [enabling and disabling](#) them, [rotating](#) [their cryptographic material](#), [adding tags](#), [creating aliases](#) that refer to the CMK, and [scheduling the CMKs for deletion](#).

For this scenario, the solutions architect should use SSE-KMS with a customer managed CMK. That way KMS will manage the data key but the company can configure key policies defining who can access the keys.

CORRECT: "Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)" is the correct answer.

INCORRECT: "Server-Side Encryption with keys stored in an S3 bucket" is incorrect as you cannot store your keys in a bucket with server-side encryption

INCORRECT: "Server-Side Encryption with Customer-Provided Keys (SSE-C)" is incorrect as the company does not want to manage the keys.

INCORRECT: "Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)" is incorrect as the company needs to manage access control for the keys which is not possible when they're managed by Amazon.

References:

<https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse>

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-kms/>

QUESTION 11

A company has some statistical data stored in an Amazon RDS database. The company want to allow users to access this information using an API. A solutions architect must create a solution that allows sporadic access to the data, ranging from no requests to large bursts of traffic.

Which solution should the solutions architect suggest?

1. Set up an Amazon API Gateway and use Amazon ECS
2. Set up an Amazon API Gateway and use AWS Elastic Beanstalk
3. Set up an Amazon API Gateway and use AWS Lambda functions
4. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling

Answer: 3

Explanation:

This question is simply asking you to work out the best compute service for the stated requirements. The key requirements are that the compute service should be suitable for a workload that can range quite broadly in demand from no requests to large bursts of traffic.

AWS Lambda is an ideal solution as you pay only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.

CORRECT: "Set up an Amazon API Gateway and use AWS Lambda functions" is the correct answer.

INCORRECT: "Set up an Amazon API Gateway and use Amazon ECS" is incorrect

INCORRECT: "Set up an Amazon API Gateway and use AWS Elastic Beanstalk" is incorrect

INCORRECT: "Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling" is incorrect

References:

<https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

QUESTION 12

A company runs a financial application using an Amazon EC2 Auto Scaling group behind an Application Load Balancer (ALB). When running month-end reports on a specific day and time each month the application becomes unacceptably slow. Amazon CloudWatch metrics show the CPU utilization hitting 100%.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

1. Configure an Amazon CloudFront distribution in front of the ALB
2. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization
3. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule
4. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances

Answer: 3

Explanation:

Scheduled scaling allows you to set your own scaling schedule. In this case the scaling action can be scheduled to occur just prior to the time that the reports will be run each month. Scaling actions are performed automatically as a function of time and date. This will ensure that there are enough EC2 instances to serve the demand and prevent the application from slowing down.

CORRECT: "Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule" is the correct answer.

INCORRECT: "Configure an Amazon CloudFront distribution in front of the ALB" is incorrect as this would be more suitable for providing access to global users by caching content.

INCORRECT: "Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization" is incorrect as this would not prevent the slow-down from occurring as there would be a delay between when the CPU hits 100% and the metric being reported and additional instances being launched.

INCORRECT: "Configure Amazon ElastiCache to remove some of the workload from the EC2 instances" is incorrect as ElastiCache is a database cache, it cannot replace the compute functions of an EC2 instance.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 13

A solutions architect is designing a high performance computing (HPC) application using Amazon EC2 Linux instances. All EC2 instances need to communicate to each other with low latency and high throughput network performance.

Which EC2 solution **BEST** meets these requirements?

1. Launch the EC2 instances in a cluster placement group in one Availability Zone
2. Launch the EC2 instances in a spread placement group in one Availability Zone
3. Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances
4. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

Answer: 1

Explanation:

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use *placement groups* to influence the placement of a group of *interdependent* instances to meet the needs of your workload. Depending on the type of workload, you can create a placement group using one of the following placement strategies:

- *Cluster* – packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.
- *Partition* – spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.

- *Spread* – strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

For this scenario, a cluster placement group should be used as this is the best option for providing low-latency network performance for a HPC application.

CORRECT: "Launch the EC2 instances in a cluster placement group in one Availability Zone" is the correct answer.

INCORRECT: "Launch the EC2 instances in a spread placement group in one Availability Zone" is incorrect as the spread placement group is used to spread instances across distinct underlying hardware.

INCORRECT: "Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances" is incorrect as this does not achieve the stated requirement to provide low-latency, high throughput network performance between instances. Also, you cannot use an ELB across Regions.

INCORRECT: "Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones" is incorrect as this does not reduce network latency or improve performance.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 14

A web application in a three-tier architecture runs on a fleet of Amazon EC2 instances. Performance issues have been reported and investigations point to insufficient swap space. The operations team requires monitoring to determine if this is correct.

What should a solutions architect recommend?

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

Answer: 3

Explanation:

You can use the CloudWatch agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers. The agent supports both Windows Server and Linux, and enables you to select the metrics to be collected, including sub-resource metrics such as per-CPU core.

There is now a unified agent and previously there were monitoring scripts. Both of these tools can capture SwapUtilization metrics and send them to CloudWatch. This is the best way to get memory utilization metrics from Amazon EC2 instances.

CORRECT: "Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch" is the correct answer.

INCORRECT: "Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch" is incorrect as you do not create custom metrics in the console, you must configure the instances to send the metric information to CloudWatch.

INCORRECT: "Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch" is incorrect as there is no SwapUsage metric in CloudWatch. All memory metrics must be custom metrics.

INCORRECT: "Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch" is incorrect as performance related information is not stored in metadata.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html>

Save time with our exam-specific cheat sheets:

QUESTION 15

A gaming company collects real-time data and stores it in an on-premises database system. The company are migrating to AWS and need better performance for the database. A solutions architect has been asked to recommend an in-memory database that supports data replication.

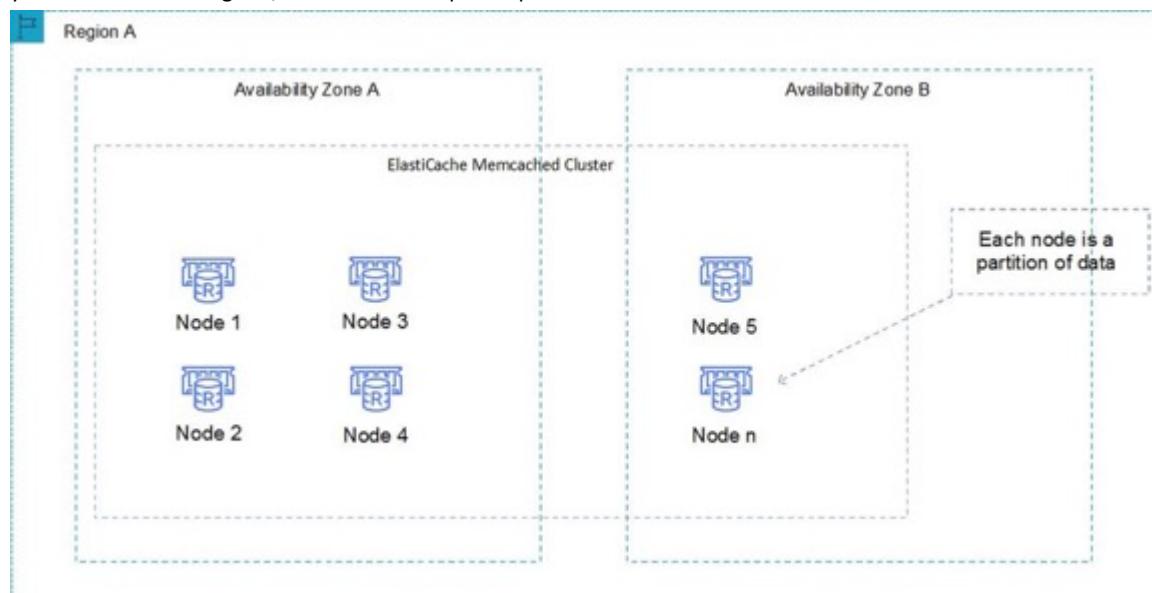
Which database should a solutions architect recommend?

1. Amazon RDS for MySQL
2. Amazon RDS for PostgreSQL
3. Amazon ElastiCache for Redis
4. Amazon ElastiCache for Memcached

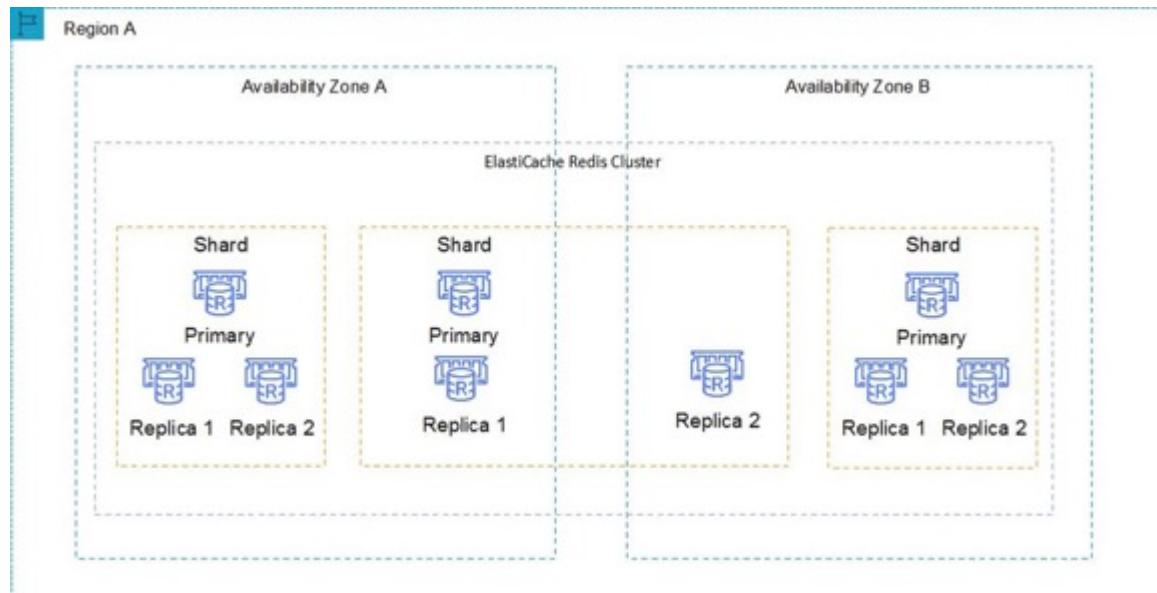
Answer: 3

Explanation:

Amazon ElastiCache is an in-memory database. With ElastiCache Memcached there is no data replication or high availability. As you can see in the diagram, each node is a separate partition of data:



Therefore, the Redis engine must be used which does support both data replication and clustering. The following diagram shows a Redis architecture with cluster mode enabled:



CORRECT: "Amazon ElastiCache for Redis" is the correct answer.

INCORRECT: "Amazon ElastiCache for Memcached" is incorrect as Memcached does not support data replication or high availability.

INCORRECT: "Amazon RDS for MySQL" is incorrect as this is not an in-memory database.

INCORRECT: "Amazon RDS for PostgreSQL" is incorrect as this is not an in-memory database.

References:

<https://aws.amazon.com/elasticsearch/redis/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticsearch/>

QUESTION 16

A company has experienced malicious traffic from some suspicious IP addresses. The security team discovered the requests are from different IP addresses under the same CIDR range.

What should a solutions architect recommend to the team?

1. Add a rule in the inbound table of the security group to deny the traffic from that CIDR range
2. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range
3. Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules
4. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules

Answer: 3

Explanation:

You can only create deny rules with network ACLs, it is not possible with security groups. Network ACLs process rules in order from the lowest numbered rules to the highest until they reach and allow or deny. The following table describes some of the differences between security groups and network ACLs:

Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

Therefore, the solutions architect should add a deny rule in the inbound table of the network ACL with a lower rule number than other rules.

CORRECT: "Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules" is the correct answer.

INCORRECT: "Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules" is incorrect as this will only block outbound traffic.

INCORRECT: "Add a rule in the inbound table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.

INCORRECT: "Add a rule in the outbound table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 17

A solutions architect is designing a microservices architecture. AWS Lambda will store data in an Amazon DynamoDB table named Orders. The solutions architect needs to apply an IAM policy to the Lambda function's execution role to allow it to put, update, and delete items in the Orders table. No other actions should be allowed.

Which of the following code snippets should be included in the IAM policy to fulfill this requirement whilst providing the LEAST privileged access?

1.


```

"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Allow",
"Action": [
    "dynamodb:PutItem",
    "dynamodb:UpdateItem",
    "dynamodb:DeleteItem"
],

```

```

    "Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"

2.
  "Sid": "PutUpdateDeleteOnOrders",
  "Effect": "Allow",
  "Action": [
    "dynamodb:PutItem",
    "dynamodb:UpdateItem",
    "dynamodb:DeleteItem"
  ],
  "Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/*"

3.

  "Sid": "PutUpdateDeleteOnOrders",
  "Effect": "Allow",
  "Action": "dynamodb:*",
  "Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"

4.
  "Sid": "PutUpdateDeleteOnOrders",
  "Effect": "Deny",
  "Action": "dynamodb:*",
  "Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"

```

Answer: 1

Explanation:

The key requirements are to allow the Lambda function the put, update, and delete actions on a single table. Using the principle of least privilege the answer should not allow any other access.

CORRECT: The following answer is correct:

```

  "Sid": "PutUpdateDeleteOnOrders",
  "Effect": "Allow",
  "Action": [
    "dynamodb:PutItem",
    "dynamodb:UpdateItem",
    "dynamodb:DeleteItem"
  ],
  "Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"

```

This code snippet specifies the exact actions to allow and also specified the resource to apply those permissions to.

INCORRECT: the following answer is incorrect:

```

  "Sid": "PutUpdateDeleteOnOrders",
  "Effect": "Allow",
  "Action": [
    "dynamodb:PutItem",
    "dynamodb:UpdateItem",
  ]

```

```
"dynamodb>DeleteItem"
],
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/*"
```

This code snippet specifies the correct list of actions but it provides a wildcard “*” instead of specifying the exact resource. Therefore, the function will be able to put, update, and delete items on any table in the account.

INCORRECT: the following answer is incorrect:

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Allow",
>Action": "dynamodb:*",
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```

This code snippet allows any action on DynamoDB by using a wildcard “dynamodb:*. This does not follow the principle of least privilege.

INCORRECT: the following answer is incorrect:

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Deny",
>Action": "dynamodb:*",
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```

This code snippet denies any action on the table. This does not have the desired effect.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 18

A company has created a duplicate of its environment in another AWS Region. The application is running in warm standby mode. There is an Application Load Balancer (ALB) in front of the application. Currently, failover is manual and requires updating a DNS alias record to point to the secondary ALB.

How can a solutions architect automate the failover process?

1. Enable an ALB health check
2. Enable an Amazon Route 53 health check
3. Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint
4. Create a latency based routing policy on Amazon Route 53

Answer: 2

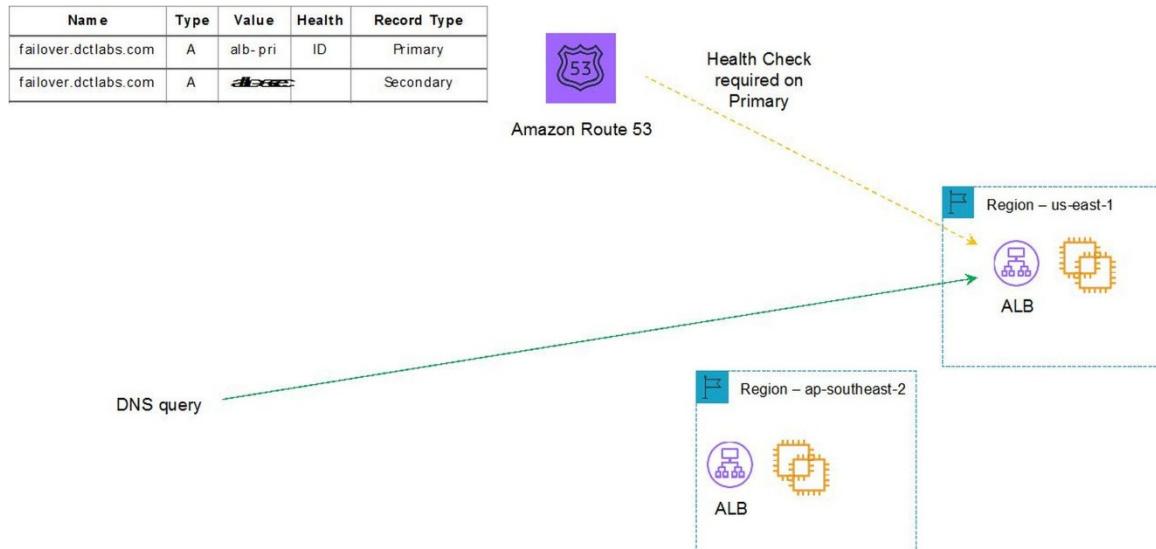
Explanation:

You can use Route 53 to check the health of your resources and only return healthy resources in response to DNS queries. There are three types of DNS failover configurations:

1. Active-passive: Route 53 actively returns a primary resource. In case of failure, Route 53 returns the backup resource. Configured using a failover policy.
2. Active-active: Route 53 actively returns more than one resource. In case of failure, Route 53 fails back to the healthy resource. Configured using any routing policy besides failover.
3. Combination: Multiple routing policies (such as latency-based, weighted, etc.) are combined into a tree to configure more complex DNS failover.

In this case an alias already exists for the secondary ALB. Therefore, the solutions architect just needs to enable a failover configuration with an Amazon Route 53 health check.

The configuration would look something like this:



CORRECT: "Enable an Amazon Route 53 health check" is the correct answer.

INCORRECT: "Enable an ALB health check" is incorrect. The point of an ALB health check is to identify the health of targets (EC2 instances). It cannot redirect clients to another Region.

INCORRECT: "Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint" is incorrect as an Alias record already exists and is better for mapping to an ALB.

INCORRECT: "Create a latency based routing policy on Amazon Route 53" is incorrect as this will only take into account latency, it is not used for failover.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

QUESTION 19

An application allows users to upload and download files. Files older than 2 years will be accessed less frequently. A solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend?

1. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard Infrequent Access (S3 Standard-IA)
2. Store the files on Amazon Elastic File System (EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA)
3. Store the files in Amazon Elastic Block Store (EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years
4. Store the files in Amazon Elastic Block Store (EBS) volumes. Create a lifecycle policy to move files older than 2 years to Amazon S3 Glacier

Answer: 1

Explanation:

S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files.

CORRECT: "Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard Infrequent

Access (S3 Standard-IA)" is the correct answer.

INCORRECT: "Store the files on Amazon Elastic File System (EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA)" is incorrect. With EFS you can transition files to EFS IA after a file has not been accessed for a specified period of time with options up to 90 days. You cannot transition based on an age of 2 years.

INCORRECT: "Store the files in Amazon Elastic Block Store (EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years" is incorrect. You cannot identify the age of data and archive snapshots in this way with EBS.

INCORRECT: "Store the files in Amazon Elastic Block Store (EBS) volumes. Create a lifecycle policy to move files older than 2 years to Amazon S3 Glacier" is incorrect. You cannot archive files from an EBS volume to Glacier using lifecycle policies.

References:

<https://aws.amazon.com/s3/storage-classes/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 20

A company is planning to migrate a large quantity of important data to Amazon S3. The data will be uploaded to a versioning enabled bucket in the us-west-1 Region. The solution needs to include replication of the data to another Region for disaster recovery purposes.

How should a solutions architect configure the replication?

1. Create an additional S3 bucket in another Region and configure cross-Region replication
2. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)
3. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication
4. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)

Answer: 3

Explanation:

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region. Both source and destination buckets must have versioning enabled.

CORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-Region replication" is the correct answer.

INCORRECT: "Create an additional S3 bucket in another Region and configure cross-Region replication" is incorrect as the destination bucket must also have versioning enabled.

INCORRECT: "Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication.

INCORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 21

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?

1. Use a simple scaling policy to dynamically scale the Auto Scaling group

2. Use a target tracking policy to dynamically scale the Auto Scaling group
3. Use an AWS Lambda function to update the desired Auto Scaling group capacity
4. Use scheduled scaling actions to scale up and scale down the Auto Scaling group

Answer: 2

Explanation:

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value.

The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to the changes in the metric due to a changing load pattern.

CORRECT: "Use a target tracking policy to dynamically scale the Auto Scaling group" is the correct answer.

INCORRECT: "Use a simple scaling policy to dynamically scale the Auto Scaling group" is incorrect as target tracking is a better way to keep the aggregate CPU usage at around 40%

INCORRECT: "Use an AWS Lambda function to update the desired Auto Scaling group capacity" is incorrect as this can be done automatically.

INCORRECT: "Use scheduled scaling actions to scale up and scale down the Auto Scaling group" is incorrect as dynamic scaling is required to respond to changes in utilization.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 22

A High Performance Computing (HPC) application needs storage that can provide 135,000 IOPS. The storage layer is replicated across all instances in a cluster.

What is the optimal storage solution that provides the required performance and is cost-effective?

1. Use Amazon EBS Provisioned IOPS volume with 135,000 IOPS
2. Use Amazon Instance Store
3. Use Amazon S3 with byte-range fetch
4. Use Amazon EC2 Enhanced Networking with an EBS HDD Throughput Optimized volume

Answer: 2

Explanation:

Instance stores offer very high performance and low latency. As long as you can afford to lose an instance, i.e. you are replicating your data, these can be a good solution for high performance/low latency requirements. Also, the cost of instance stores is included in the instance charges so it can also be more cost-effective than EBS Provisioned IOPS.

CORRECT: "Use Amazon Instance Store" is the correct answer.

INCORRECT: "Use Amazon EBS Provisioned IOPS volume with 135,000 IOPS" is incorrect. In the case of a HPC cluster that replicates data between nodes you don't necessarily need a shared storage solution such as Amazon EBS Provisioned IOPS – this would also be a more expensive solution as the Instance Store is included in the cost of the HPC instance.

INCORRECT: "Use Amazon S3 with byte-range fetch" is incorrect. Amazon S3 is not a solution for this HPC application as in this case it will require block-based storage to provide the required IOPS.

INCORRECT: "Enhanced networking provides higher bandwidth and lower latency and is implemented using an Elastic Network Adapter (ENA). However, using an ENA with an HDD Throughput Optimized volume is not recommended and the volume will not provide the performance required for this use case." is incorrect

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 23

A high-performance file system is required for a financial modelling application. The data set will be stored on Amazon S3 and the storage solution must have seamless integration so objects can be accessed as files.

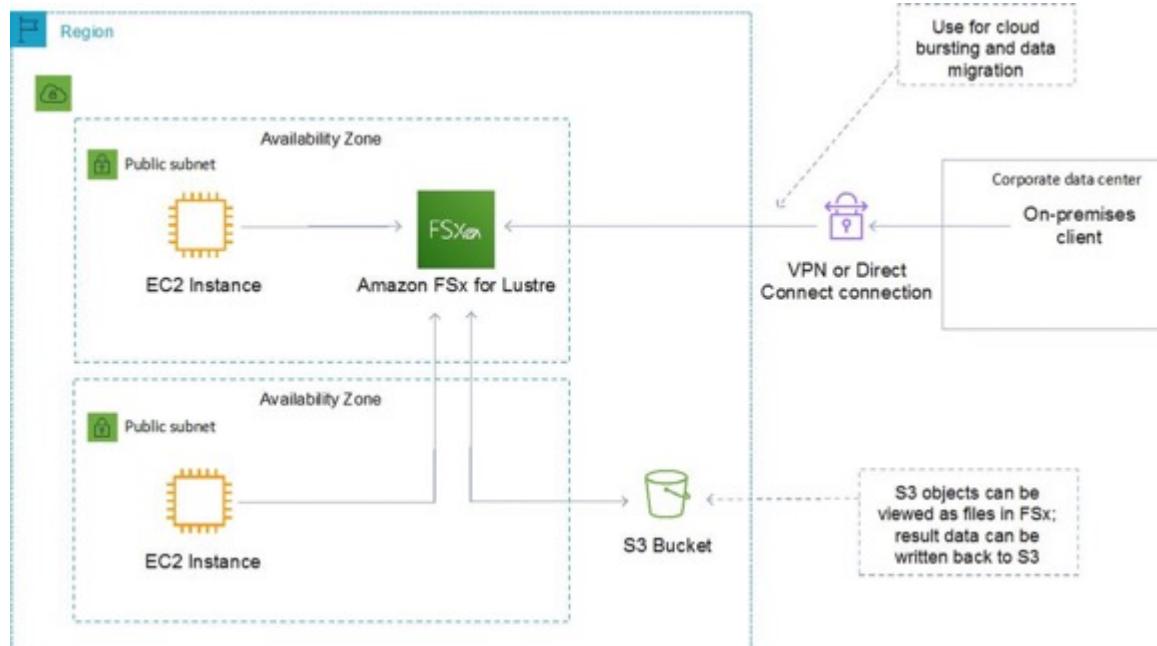
Which storage solution should be used?

1. Amazon FSx for Windows File Server
2. Amazon FSx for Lustre
3. Amazon Elastic File System (EFS)
4. Amazon Elastic Block Store (EBS)

Answer: 2

Explanation:

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA). Amazon FSx works natively with Amazon S3, letting you transparently access your S3 objects as files on Amazon FSx to run analyses for hours to months.



CORRECT: "Amazon FSx for Lustre" is the correct answer.

INCORRECT: "Amazon FSx for Windows File Server" is incorrect. Amazon FSx for Windows File Server provides a fully managed native Microsoft Windows file system so you can easily move your Windows-based applications that require shared file storage to AWS. This solution integrates with Windows file shares, not with Amazon S3.

INCORRECT: "Amazon Elastic File System (EFS)" is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.

INCORRECT: "Amazon Elastic Block Store (EBS)" is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.

References:

<https://aws.amazon.com/fsx/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 24

An application requires a MySQL database which will only be used several times a week for short periods. The database needs to provide automatic instantiation and scaling. Which database service is most suitable?

1. Amazon RDS MySQL
2. Amazon EC2 instance with MySQL database installed
3. Amazon Aurora
4. Amazon Aurora Serverless

Answer: 4

Explanation:

Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora. The database automatically starts up, shuts down, and scales capacity up or down based on application needs. This is an ideal database solution for infrequently-used applications.

CORRECT: "Amazon Aurora Serverless" is the correct answer.

INCORRECT: "Amazon RDS MySQL" is incorrect as this service requires an instance to be running all the time which is more costly.

INCORRECT: "Amazon EC2 instance with MySQL database installed" is incorrect as this service requires an instance to be running all the time which is more costly.

INCORRECT: "Amazon Aurora" is incorrect as this service requires an instance to be running all the time which is more costly.

References:

<https://aws.amazon.com/rds/aurora/serverless/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>

QUESTION 25

An Architect needs to find a way to automatically and repeatably create many member accounts within an AWS Organization. The accounts also need to be moved into an OU and have VPCs and subnets created.

What is the best way to achieve this?

1. Use the AWS Organizations API
2. Use CloudFormation with scripts
3. Use the AWS Management Console
4. Use the AWS CLI

Answer: 2

Explanation:

The best solution is to use a combination of scripts and AWS CloudFormation. You will also leverage the AWS Organizations API. This solution can provide all of the requirements.

CORRECT: "Use CloudFormation with scripts" is the correct answer.

INCORRECT: "Use the AWS Organizations API" is incorrect. You can create member accounts with the AWS Organizations API. However, you cannot use that API to configure the account and create VPCs and subnets.

INCORRECT: "Use the AWS Management Console" is incorrect. Using the AWS Management Console is not a method of automatically creating the resources.

INCORRECT: "Use the AWS CLI" is incorrect. You can do all tasks using the AWS CLI but it is better to automate the process using AWS CloudFormation.

References:

<https://aws.amazon.com/blogs/security/how-to-use-aws-organizations-to-automate-end-to-end-account-creation/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-organizations/>

QUESTION 26

An organization is extending a secure development environment into AWS. They have already secured the VPC including removing the Internet Gateway and setting up a Direct Connect connection. What else needs to be done to add encryption?

1. Setup a Virtual Private Gateway (VPG)
2. Enable IPSec encryption on the Direct Connect connection
3. Setup the Border Gateway Protocol (BGP) with encryption
4. Configure an AWS Direct Connect Gateway

Answer: 1

Explanation:

A VPG is used to setup an AWS VPN which you can use in combination with Direct Connect to encrypt all data that traverses the Direct Connect link. This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.

CORRECT: "Setup a Virtual Private Gateway (VPG)" is the correct answer.

INCORRECT: "Enable IPSec encryption on the Direct Connect connection" is incorrect. There is no option to enable IPSec encryption on the Direct Connect connection.

INCORRECT: "Setup the Border Gateway Protocol (BGP) with encryption" is incorrect. The BGP protocol is not used to enable encryption for Direct Connect, it is used for routing.

INCORRECT: "Configure an AWS Direct Connect Gateway" is incorrect. An AWS Direct Connect Gateway is used to connect to VPCs across multiple AWS regions. It is not involved with encryption.

References:

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html>

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 27

A shared services VPC is being setup for use by several AWS accounts. An application needs to be securely shared from the shared services VPC. The solution should not allow consumers to connect to other instances in the VPC.

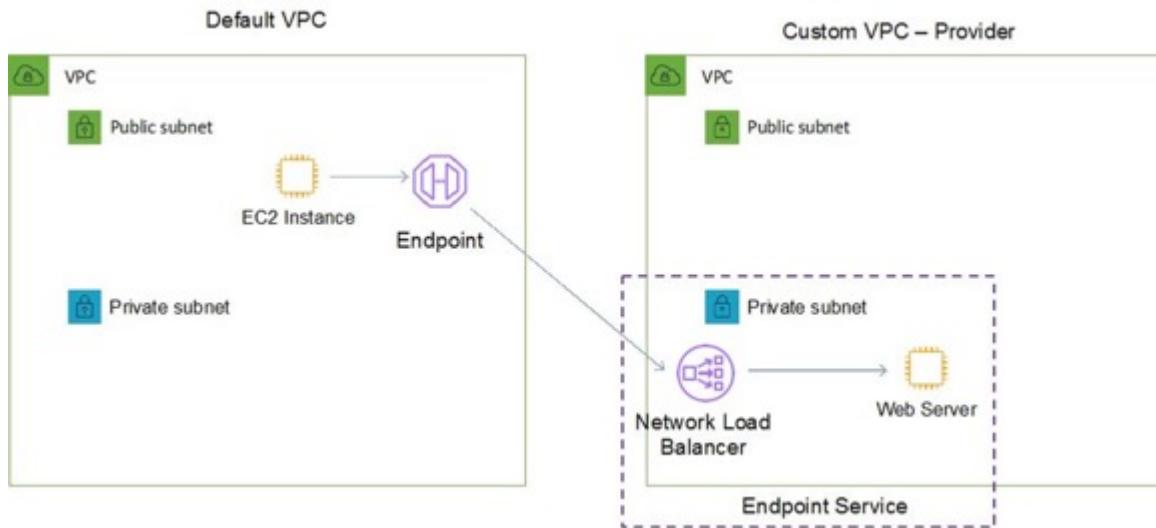
How can this be setup with the least administrative effort? (Select TWO.)

1. Create a Network Load Balancer (NLB)
2. Use AWS PrivateLink to expose the application as an endpoint service
3. Use AWS ClassicLink to expose the application as an endpoint service
4. Setup VPC peering between each AWS VPC
5. Configure security groups to restrict access

Answer: 1,2

Explanation:

VPCs can be shared among multiple AWS accounts. Resources can then be shared amongst those accounts. However, to restrict access so that consumers cannot connect to other instances in the VPC the best solution is to use PrivateLink to create an endpoint for the application. The endpoint type will be an interface endpoint and it uses an NLB in the shared services VPC.



CORRECT: "Create a Network Load Balancer (NLB)" is a correct answer.

CORRECT: "Use AWS PrivateLink to expose the application as an endpoint service" is also a correct answer.

INCORRECT: "Use AWS ClassicLink to expose the application as an endpoint service" is incorrect. ClassicLink allows you to link EC2-Classic instances to a VPC in your account, within the same region. This solution does not include EC2-Classic which is now deprecated (replaced by VPC).

INCORRECT: "Setup VPC peering between each AWS VPC" is incorrect. VPC peering could be used along with security groups to restrict access to the application and other instances in the VPC. However, this would be administratively difficult as you would need to ensure that you maintain the security groups as resources and addresses change.

INCORRECT: "Configure security groups to restrict access" is incorrect. This could be used in conjunction with VPC peering but better method is to use PrivateLink for this use case.

References:

<https://aws.amazon.com/about-aws/whats-new/2018/12/amazon-virtual-private-clouds-can-now-be-shared-with-other-aws-accounts/>

<https://aws.amazon.com/blogs/networking-and-content-delivery/vpc-sharing-a-new-approach-to-multiple-accounts-and-vpc-management/>

<https://d1.awsstatic.com/whitepapers/aws-privatelink.pdf>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 28

A web app allows users to upload images for viewing online. The compute layer that processes the images is behind an Auto Scaling group. The processing layer should be decoupled from the front end and the ASG needs to dynamically adjust based on the number of images being uploaded.

How can this be achieved?

1. Create an Amazon SNS Topic to generate a notification each time a message is uploaded. Have the ASG scale based on the number of SNS messages
2. Create a target tracking policy that keeps the ASG at 70% CPU utilization
3. Create an Amazon SQS queue and custom CloudWatch metric to measure the number of messages in the queue. Configure the ASG to scale based on the number of messages in the queue
4. Create a scheduled policy that scales the ASG at times of expected peak load

Answer: 3

Explanation:

The best solution is to use Amazon SQS to decouple the front end from the processing compute layer. To do this you can create a custom CloudWatch metric that measures the number of messages in the queue and then configure the ASG to scale using a target tracking policy that tracks a certain value.

CORRECT: "Create an Amazon SQS queue and custom CloudWatch metric to measure the number of messages in the queue. Configure the ASG to scale based on the number of messages in the queue" is the correct answer.

INCORRECT: "Create an Amazon SNS Topic to generate a notification each time a message is uploaded. Have the ASG scale based on the number of SNS messages" is incorrect. The Amazon Simple Notification Service (SNS) is used for sending notifications using topics. Amazon SQS is a better solution for this scenario as it provides a decoupling mechanism where the actual images can be stored for processing. SNS does not provide somewhere for the images to be stored.

INCORRECT: "Create a target tracking policy that keeps the ASG at 70% CPU utilization" is incorrect. Using a target tracking policy with the ASG that tracks CPU utilization does not allow scaling based on the number of images being uploaded.

INCORRECT: "Create a scheduled policy that scales the ASG at times of expected peak load" is incorrect. Using a scheduled policy is less dynamic as though you may be able to predict usage patterns, it would be better to adjust dynamically based on actual usage.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 29

A web application is running on a fleet of Amazon EC2 instances using an Auto Scaling Group. It is desired that the CPU usage in the fleet is kept at 40%.

How should scaling be configured?

1. Use a simple scaling policy that launches instances when the average CPU hits 40%
2. Use a target tracking policy that keeps the average aggregate CPU utilization at 40%
3. Use a step scaling policy that uses the PercentChangeInCapacity value to adjust the group size as required
4. Use a custom CloudWatch alarm to monitor CPU usage and notify the ASG using Amazon SNS

Answer: 2

Explanation:

This is a perfect use case for a target tracking scaling policy. With target tracking scaling policies, you select a scaling metric and set a target value. In this case you can just set the target value to 40% average aggregate CPU utilization.

CORRECT: "Use a target tracking policy that keeps the average aggregate CPU utilization at 40%" is the correct answer.

INCORRECT: "Use a simple scaling policy that launches instances when the average CPU hits 40%" is incorrect. A simple scaling policy will add instances when 40% CPU utilization is reached, but it is not designed to maintain 40% CPU utilization across the group.

INCORRECT: "Use a step scaling policy that uses the PercentChangeInCapacity value to adjust the group size as required" is incorrect. The step scaling policy makes scaling adjustments based on a number of factors. The PercentChangeInCapacity value increments or decrements the group size by a specified percentage. This does not relate to CPU utilization.

INCORRECT: "Use a custom CloudWatch alarm to monitor CPU usage and notify the ASG using Amazon SNS" is incorrect. You do not need to create a custom Amazon CloudWatch alarm as the ASG can scale using a policy based on CPU utilization using standard configuration.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

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

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 30

Health related data in Amazon S3 needs to be frequently accessed for up to 90 days. After that time the data must be retained for compliance reasons for seven years and is rarely accessed.

Which storage classes should be used?

1. Store data in STANDARD for 90 days then transition the data to DEEP_ARCHIVE
2. Store data in INTELLIGENT_TIERING for 90 days then transition to STANDARD_IA
3. Store data in STANDARD for 90 days then expire the data
4. Store data in STANDARD for 90 days then transition to REDUCED_REDUNDANCY

Answer: 1

Explanation:

In this case the data is frequently accessed so must be stored in standard for the first 90 days. After that the data is still to be kept for compliance reasons but is rarely accessed so is a good use case for DEEP_ARCHIVE.

CORRECT: "Store data in STANDARD for 90 days then transition the data to DEEP_ARCHIVE" is the correct answer.

INCORRECT: "Store data in INTELLIGENT_TIERING for 90 days then transition to STANDARD_IA" is incorrect. You cannot transition from INTELLIGENT_TIERING to STANDARD_IA.

INCORRECT: "Store data in STANDARD for 90 days then expire the data" is incorrect. Expiring the data is not possible as it must be retained for compliance.

INCORRECT: "Store data in STANDARD for 90 days then transition to REDUCED_REDUNDANCY" is incorrect. You cannot transition from any storage class to REDUCED_REDUNDANCY.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 31

An e-commerce web application needs a highly scalable key-value database. Which AWS database service should be used?

1. Amazon RDS
2. Amazon RedShift
3. Amazon DynamoDB
4. Amazon ElastiCache

Answer: 3

Explanation:

A key-value database is a type of nonrelational (NoSQL) database that uses a simple key-value method to store data. A key-value database stores data as a collection of key-value pairs in which a key serves as a unique identifier. Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability – this is the best database for these requirements.

CORRECT: "Amazon DynamoDB" is the correct answer.

INCORRECT: "Amazon RDS" is incorrect. Amazon RDS is a relational (SQL) type of database, not a key-value / nonrelational database.

INCORRECT: "Amazon RedShift" is incorrect. Amazon RedShift is a data warehouse service used for online analytics processing (OLAP) workloads.

INCORRECT: "Amazon ElastiCache" is incorrect. Amazon ElastiCache is an in-memory caching database. This is not a nonrelational key-value database.

References:

<https://aws.amazon.com/nosql/key-value/>

Save time with our exam-specific cheat sheets:

QUESTION 32

A Solutions Architect is designing a mobile application that will capture receipt images to track expenses. The Architect wants to store the images on Amazon S3. However, uploading the images through the web server will create too much traffic.

What is the MOST efficient method to store images from a mobile application on Amazon S3?

1. Expand the web server fleet with Spot instances to provide the resources to handle the images
2. Upload to a second bucket, and have a Lambda event copy the image to the primary bucket
3. Upload to a separate Auto Scaling Group of server behind an ELB Classic Load Balancer, and have the server instances write to the Amazon S3 bucket
4. Upload directly to S3 using a pre-signed URL

Answer: 4

Explanation:

Uploading using a pre-signed URL allows you to upload the object without having any AWS security credentials/permissions. Pre-signed URLs can be generated programmatically and anyone who receives a valid pre-signed URL can then programmatically upload an object. This solution bypasses the web server avoiding any performance bottlenecks.

CORRECT: "Upload directly to S3 using a pre-signed URL" is the correct answer.

INCORRECT: "Expand the web server fleet with Spot instances to provide the resources to handle the images" is incorrect as this is not the most efficient solution.

INCORRECT: "Upload to a second bucket, and have a Lambda event copy the image to the primary bucket" is incorrect. Uploading to a second bucket (through the web server) does not solve the issue of the web server being the bottleneck.

INCORRECT: "Upload to a separate Auto Scaling Group of server behind an ELB Classic Load Balancer, and have the server instances write to the Amazon S3 bucket" is incorrect as this is not the most efficient solution.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 33

A Kinesis consumer application is reading at a slower rate than expected. It has been identified that multiple consumer applications have total reads exceeding the per-shard limits. How can this situation be resolved?

1. Increase the number of shards in the Kinesis data stream
2. Implement API throttling to restrict the number of requests per-shard
3. Increase the number of read transactions per shard
4. Implement read throttling for the Kinesis data stream

Answer: 1

Explanation:

One shard provides a capacity of 1MB/sec data input and 2MB/sec data output. One shard can support up to 1000 PUT records per second. The total capacity of the stream is the sum of the capacities of its shards.

In a case where multiple consumer applications have total reads exceeding the per-shard limits, you need to increase the number of shards in the Kinesis data stream.

CORRECT: "Increase the number of shards in the Kinesis data stream" is the correct answer.

INCORRECT: "Implement API throttling to restrict the number of requests per-shard" is incorrect. API throttling is used to throttle API requests it is not responsible and cannot be used for throttling Get requests in a Kinesis stream.

INCORRECT: "Increase the number of read transactions per shard" is incorrect. You cannot increase the number of read transactions per shard. Read throttling is enabled by default for Kinesis data streams. If you're still experiencing performance issues you must increase the number of shards.

INCORRECT: "Implement read throttling for the Kinesis data stream" is incorrect

References:

<https://docs.aws.amazon.com/streams/latest/dev/troubleshooting-consumers.html#consumer-app-reading-slower>

<https://docs.aws.amazon.com/streams/latest/dev/kinesis-record-processor-additional-considerations.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>

QUESTION 34

You need to scale read operations for your Amazon Aurora DB within a region. To increase availability you also need to be able to failover if the primary instance fails.

What should you implement?

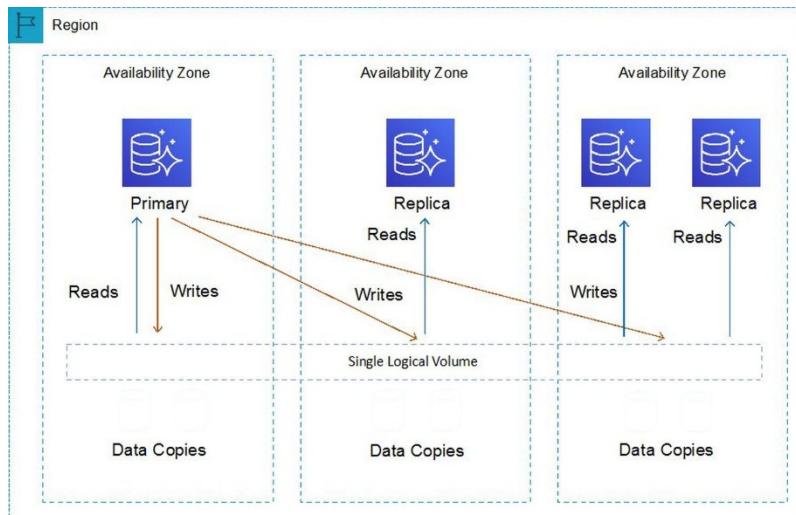
1. Aurora Replicas
2. A DB cluster
3. An Aurora Cluster Volume
4. Aurora Global Database

Answer: 1

Explanation:

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region. To increase availability, you can use Aurora Replicas as failover targets. That is, if the primary instance fails, an Aurora Replica is promoted to the primary instance.

The graphic below provides an overview of Aurora Replicas:



CORRECT: "Aurora Replicas" is the correct answer.

INCORRECT: "A DB cluster" is incorrect. An **Amazon Aurora DB cluster** consists of a DB instance, compatible with either MySQL or PostgreSQL, and a cluster volume that represents the data for the DB cluster, copied across three Availability Zones as a single, virtual volume. The DB cluster contains a primary instance and, *optionally*, up to 15 Aurora Replicas. A DB cluster does not necessarily scale read operations as it is option to deploy Aurora Replicas, therefore it can be thought of as more of a storage level availability feature in this case and is not the best answer.

INCORRECT: "An Aurora Cluster Volume" is incorrect. A cluster volume manages the data for DB instances in a DB cluster and does not provide read scaling.

INCORRECT: "Aurora Global Database" is incorrect. Amazon Aurora Global Database is not suitable for scaling read operations within a region. It is a new feature in the MySQL-compatible edition of Amazon Aurora, designed for applications with a global

footprint. It allows a single Aurora database to span multiple AWS regions, with fast replication to enable low-latency global reads and disaster recovery from region-wide outages.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>

QUESTION 35

A Solutions Architect needs to monitor application logs and receive a notification whenever a specific number of occurrences of certain HTTP status code errors occur. Which tool should the Architect use?

1. CloudWatch Metrics
2. CloudWatch Events
3. CloudTrail Trails
4. CloudWatch Logs

Answer: 4

Explanation:

You can use CloudWatch Logs to monitor applications and systems using log data. For example, CloudWatch Logs can track the number of errors that occur in your application logs and send you a notification whenever the rate of errors exceeds a threshold you specify. This is the best tool for this requirement.

CORRECT: "CloudWatch Logs" is the correct answer.

INCORRECT: "CloudWatch Metrics" is incorrect. CloudWatch Metrics are the fundamental concept in CloudWatch. A metric represents a time-ordered set of data points that are published to CloudWatch. You cannot use a metric alone, it is used when setting up monitoring for any service in CloudWatch.

INCORRECT: "CloudWatch Events" is incorrect. Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Though you can generate custom application-level events and publish them to CloudWatch Events this is not the best tool for monitoring application logs.

INCORRECT: "CloudTrail Trails" is incorrect. CloudTrail is used for monitoring API activity on your account, not for monitoring application logs.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/>

QUESTION 36

An application consists of a web tier in a public subnet and a MySQL cluster hosted on Amazon EC2 instances in a private subnet. The MySQL instances must retrieve product data from a third-party provider over the internet. A Solutions Architect must determine a strategy to enable this access with maximum security and minimum operational overhead.

What should the Solutions Architect do to meet these requirements?

1. Deploy a NAT instance in the private subnet. Direct all internet traffic to the NAT instance.
2. Create an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the internet gateway.
3. Deploy a NAT gateway in the public subnet. Modify the route table in the private subnet to direct all internet traffic to the NAT gateway.
4. Create a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the virtual private gateway.

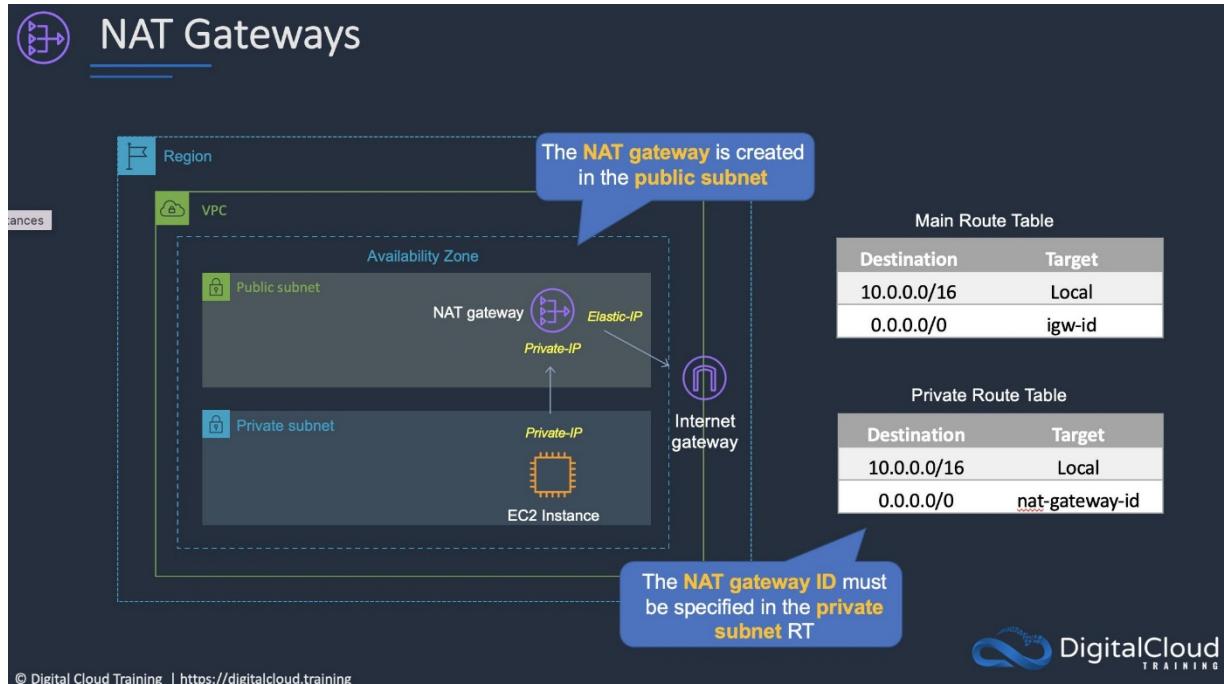
Answer: 3

Explanation:

The MySQL clusters instances need to access a service on the internet. The most secure method of enabling this access with low

operational overhead is to create a NAT gateway. When deploying a NAT gateway, the gateway itself should be deployed in a public subnet whilst the route table in the private subnet must be updated to point traffic to the NAT gateway ID.

The configuration can be seen in the diagram below:



CORRECT: "Deploy a NAT gateway in the public subnet. Modify the route table in the private subnet to direct all internet traffic to the NAT gateway" is the correct answer.

INCORRECT: "Deploy a NAT instance in the private subnet. Direct all internet traffic to the NAT instance" is incorrect. NAT instances require more operational overhead and need to be deployed in a public subnet.

INCORRECT: "Create an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the internet gateway" is incorrect. You cannot point the instances in the private subnet to an internet gateway as they do not have public IP addresses which is required to use an internet gateway.

INCORRECT: "Create a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the virtual private gateway" is incorrect. A virtual private gateway (VGW) is used with a VPN connection, not for connecting instances in private subnets to the internet.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 37

A company needs to migrate a large quantity of data from an on-premises environment to Amazon S3. The company is connected via an AWS Direct Connect (DX) connection. The company requires a fully managed solution that will keep the data private and automate and accelerate the replication of the data to AWS storage services.

Which solution should a Solutions Architect recommend?

1. Deploy an AWS Storage Gateway volume gateway in stored volume mode and take point-in-time copies of the volumes using AWS Backup.

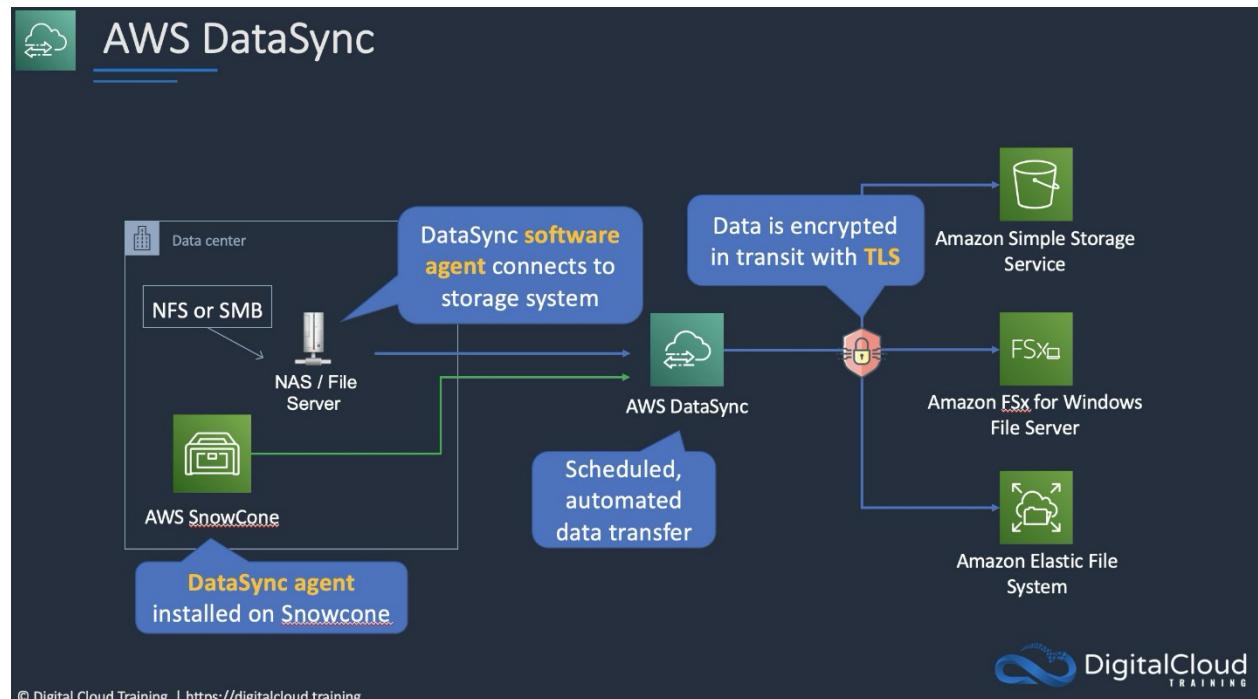
2. Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a VPC endpoint.
3. Deploy an AWS Storage Gateway file gateway with a local cache and store the primary data set in Amazon S3.
4. Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a public endpoint.

Answer: 2

Explanation:

AWS DataSync can be used to automate and accelerate the replication of data to AWS storage services. Note that Storage Gateway is used for hybrid scenarios where servers need local access to data with various options for storing and synchronizing the data to AWS storage services. Storage Gateway does not accelerate replication of data.

To deploy DataSync an agent must be installed. Then a task must be configured to replicated data to AWS. The task requires a connection to a service endpoint. To keep the data private and send it across the DX connection, a VPC endpoint should be used.



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a VPC endpoint" is the correct answer.

INCORRECT: "Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a public endpoint" is incorrect. A public endpoint will send data over the public internet which should be avoided in this scenario.

INCORRECT: "Deploy an AWS Storage Gateway volume gateway in stored volume mode and take point-in-time copies of the volumes using AWS Backup" is incorrect. Storage Gateway will not accelerate replication and a volume gateway will create EBS snapshots (not S3 objects).

INCORRECT: "Deploy an AWS Storage Gateway file gateway with a local cache and store the primary data set in Amazon S3" is incorrect. Storage Gateway will not accelerate replication and a file gateway should be used for providing NFS or CIFS/SMB access to data locally which is not required.

References:

<https://docs.aws.amazon.com/datasync/latest/userguide/choose-service-endpoint.html>

Save time with our exam-specific cheat sheets:

QUESTION 38

A company has a Production VPC and a Pre-Production VPC. The Production VPC uses VPNs through a customer gateway to connect to a single device in an on-premises data center. The Pre-Production VPC uses a virtual private gateway attached to two AWS Direct Connect (DX) connections. Both VPCs are connected using a single VPC peering connection.

How can a Solutions Architect improve this architecture to remove any single point of failure?

1. Add an additional VPC peering connection between the two VPCs.
2. Add additional VPNs to the Production VPC from a second customer gateway device.
3. Add a set of VPNs between the Production and Pre-Production VPCs.
4. Add a second virtual private gateway and attach it to the Production VPC.

Answer: 2

Explanation:

The only single point of failure in this architecture is the customer gateway device in the on-premises data center. A customer gateway device is the on-premises (client) side of the connection into the VPC. The customer gateway configuration is created within AWS, but the actual device is a physical or virtual device running in the on-premises data center. If this device is a single device, then if it fails the VPN connections will fail. The AWS side of the VPN link is the virtual private gateway, and this is a redundant device.

CORRECT: "Add additional VPNs to the Production VPC from a second customer gateway device" is the correct answer.

INCORRECT: "Add an additional VPC peering connection between the two VPCs" is incorrect. VPC peering connections are already redundant, you do not need multiple connections.

INCORRECT: "Add a set of VPNs between the Production and Pre-Production VPCs" is incorrect. You cannot create VPN connections between VPCs (using AWS VPNs).

INCORRECT: "Add a second virtual private gateway and attach it to the Production VPC" is incorrect. Virtual private gateways (VGWs) are redundant devices so a second one is not necessary.

References:

<https://docs.aws.amazon.com/vpn/latest/s2vpn/your-cgw.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 39

A Solutions Architect must design a solution to allow many Amazon EC2 instances across multiple subnets to access a shared data store. The data must be accessed by all instances simultaneously and access should use the NFS protocol. The solution must also be highly scalable and easy to implement.

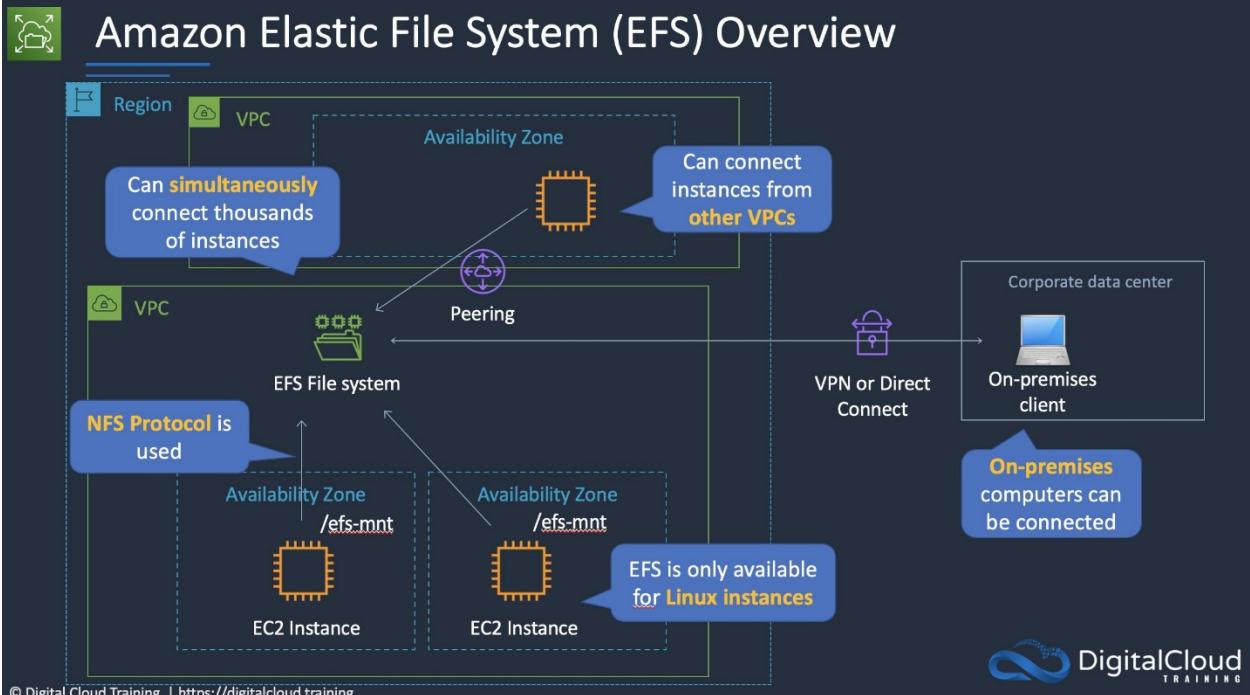
Which solution best meets these requirements?

1. Configure an additional EC2 instance as a file server. Create a role in AWS IAM that grants permissions to the file share and attach the role to the EC2 instances.
2. Create an Amazon S3 bucket and configure a Network ACL. Grant the EC2 instances permission to access the bucket using the NFS protocol.
3. Create an Amazon EBS volume and create a resource-based policy that grants an AWS IAM role access to the data. Attach the role to the EC2 instances.
4. Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.

Answer: 4

Explanation:

The Amazon Elastic File System (EFS) is a perfect solution for this requirement. Amazon EFS filesystems are accessed using the NFS protocol and can be mounted by many instances across multiple subnets simultaneously. EFS filesystems are highly scalable and very easy to implement.



CORRECT: "Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target" is the correct answer.

INCORRECT: "Configure an additional EC2 instance as a file server. Create a role in AWS IAM that grants permissions to the file share and attach the role to the EC2 instances" is incorrect. You cannot use IAM roles to grant permissions to a file share created within the operating system of an EC2 instance. Also, this solution is not as highly scalable or easy to implement as Amazon EFS.

INCORRECT: "Create an Amazon S3 bucket and configure a Network ACL. Grant the EC2 instances permission to access the bucket using the NFS protocol" is incorrect. A Network ACL is created to restrict traffic in and out of subnets, it is not used to control access to S3 buckets (use a bucket policy or bucket ACL instead). You cannot grant permission to access an S3 bucket using a protocol, and NFS is not supported for S3 as it is an object-based storage system.

INCORRECT: "Create an Amazon EBS volume and create a resource-based policy that grants an AWS IAM role access to the data. Attach the role to the EC2 instances" is incorrect. You cannot configure a resource-based policy on an Amazon EBS volume.

References:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 40

A company requires a fully managed replacement for an on-premises storage service. The company's employees often work remotely from various locations. The solution should also be easily accessible to systems connected to the on-premises environment.

Which solution meets these requirements?

1. Use AWS Transfer Acceleration to replicate files to Amazon S3 and enable public access.
2. Use Amazon FSx to create an SMB file share. Connect remote clients to the file share over a client VPN.
3. Use AWS DataSync to synchronize data between the on-premises service and Amazon S3.
4. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.

Answer: 2**Explanation:**

Amazon FSx for Windows File Server (Amazon FSx) is a fully managed, highly available, and scalable file storage solution built on Windows Server that uses the Server Message Block (SMB) protocol. It allows for Microsoft Active Directory integration, data deduplication, and fully managed backups, among other critical enterprise features.

An Amazon FSx file system can be created to host the file shares. Clients can then be connected to an AWS Client VPN endpoint and gateway to enable remote access. The protocol used in this solution will be SMB.

CORRECT: "Use Amazon FSx to create an SMB file share. Connect remote clients to the file share over a client VPN" is the correct answer.

INCORRECT: "Use AWS Transfer Acceleration to replicate files to Amazon S3 and enable public access" is incorrect. This is simply a way of improving upload speeds to S3, it is not suitable for enabling internal and external access to a file system.

INCORRECT: "Use AWS DataSync to synchronize data between the on-premises service and Amazon S3" is incorrect. The on-premises solution is to be replaced so this is not a satisfactory solution. Also, DataSync syncs one way, it is not bidirectional.

INCORRECT: "Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3" is incorrect. Storage Gateway volume gateways are mounted using block-based protocols (iSCSI), so this would not be workable.

References:

<https://aws.amazon.com/blogs/storage/accessing-smb-file-shares-remotely-with-amazon-fsx-for-windows-file-server/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 41

A company hosts statistical data in an Amazon S3 bucket that users around the world download from their website using a URL that resolves to a domain name. The company needs to provide low latency access to users and plans to use Amazon Route 53 for hosting DNS records.

Which solution meets these requirements?

1. Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
2. Create an A record in Route 53, use 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.
3. Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. 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.
4. Create an A record in Route 53, use 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: 3**Explanation:**

This is a simple requirement for low latency access to the contents of an Amazon S3 bucket for global users. The best solution here is to use Amazon CloudFront to cache the content in Edge Locations around the world. This involves creating a web distribution that points to an S3 origin (the bucket) and then create an Alias record in Route 53 that resolves the applications URL to the CloudFront distribution endpoint.

CORRECT: "Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. 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" is the correct answer.

INCORRECT: "Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name" is incorrect. An Alias record should be used to point to an Amazon CloudFront distribution.

INCORRECT: "Create an A record in Route 53, use 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" is incorrect. There is only a single endpoint (the Amazon S3 bucket) so this strategy would not work. Much better to use CloudFront to cache in multiple locations.

INCORRECT: "Create an A record in Route 53, use 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" is incorrect. Again, there is only one endpoint so this strategy will simply not work.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/RoutingToS3Bucket.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

QUESTION 42

A company requires a high-performance file system that can be mounted on Amazon EC2 Windows instances and Amazon EC2 Linux instances. Applications running on the EC2 instances perform separate processing of the same files and the solution must provide a file system that can be mounted by all instances simultaneously.

Which solution meets these requirements?

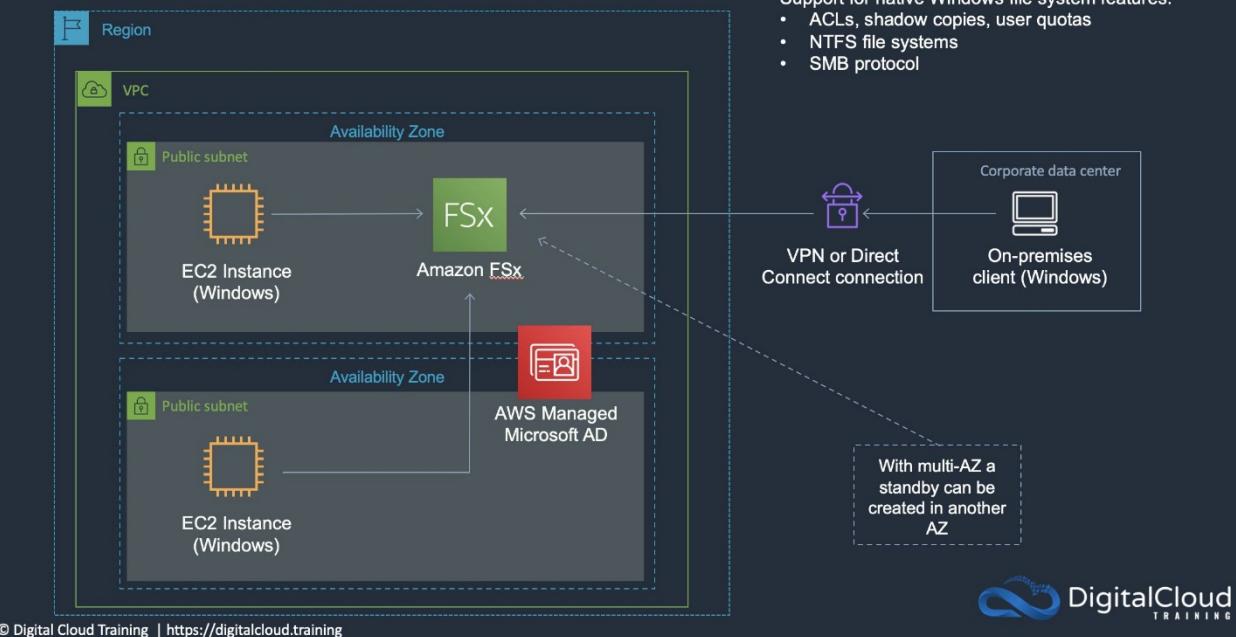
1. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances.
2. Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances.
3. Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances.
4. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket.

Answer: 3

Explanation:

Amazon FSx for Windows File Server provides a fully managed native Microsoft Windows file system so you can easily move your Windows-based applications that require shared file storage to AWS. You can easily connect Linux instances to the file system by installing the cifs-utils package. The Linux instances can then mount an SMB/CIFS file system.

Amazon FSx for Windows File Server



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances" is the correct answer.

INCORRECT: "Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances" is incorrect. This solution results in two separate file systems and a shared file system is required.

INCORRECT: "Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances" is incorrect. You cannot use Amazon EFS for Windows instances as this is not supported.

INCORRECT: "Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket" is incorrect. Amazon FSx for Windows File Server does not use Amazon S3 buckets, so this is another solution that results in separate file systems.

References:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/using-file-shares.html#map-shares-linux>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 43

A company is deploying an application that produces data that must be processed in the order it is received. The company requires a solution for decoupling the event data from the processing layer. The solution must minimize operational overhead.

How can a Solutions Architect meet these requirements?

1. Create an Amazon SQS standard queue to decouple the application. Set up an AWS Lambda function to process messages from the queue independently.
2. Create an Amazon SNS topic to decouple the application. Configure an AWS Lambda function as a subscriber.
3. Create an Amazon SQS FIFO queue to decouple the application. Configure an AWS Lambda function to process messages from the queue.
4. Create an Amazon SNS topic to decouple the application. Configure an Amazon SQS queue as a subscriber.

Answer: 3

Explanation:

Amazon SQS can be used to decouple this application using a FIFO queue. With a FIFO queue the order in which messages are

sent and received is strictly preserved. You can configure an AWS Lambda function to poll the queue, or you can configure a Lambda function as a destination to asynchronously process messages from the queue.



CORRECT: "Create an Amazon SQS FIFO queue to decouple the application. Configure an AWS Lambda function to process messages from the queue" is the correct answer.

INCORRECT: "Create an Amazon SQS standard queue to decouple the application. Set up an AWS Lambda function to process messages from the queue independently" is incorrect. A standard queue only offers best-effort ordering so it may not preserve the order of the data.

INCORRECT: "Create an Amazon SNS topic to decouple the application. Configure an AWS Lambda function as a subscriber" is incorrect. Amazon SQS is better for this use case as there are a sequence of events for which the order must be maintained, and these events can be queued for processing whereas SNS delivers them for immediate processing.

INCORRECT: "Create an Amazon SNS topic to decouple the application. Configure an Amazon SQS queue as a subscriber" is incorrect. As above an SQS queue would be preferred for queuing the messages.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-lambda-function-trigger.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 44

An application runs on-premises and produces data that must be stored in a locally accessible file system that servers can mount using the NFS protocol. The data must be subsequently analyzed by Amazon EC2 instances in the AWS Cloud.

How can these requirements be met?

1. Use an AWS Storage Gateway tape gateway to take a backup of the local data and store it on AWS, then perform analytics on this data in the AWS Cloud.
2. Use an AWS Storage Gateway volume gateway in stored mode to regularly take snapshots of the local data, then copy the data to AWS.
3. Use an AWS Storage Gateway volume gateway in cached mode to back up all the local storage in the AWS Cloud, then perform analytics on this data in the cloud.
4. Use an AWS Storage Gateway file gateway to provide a locally accessible file system that replicates data to the cloud, then analyze the data in the AWS Cloud.

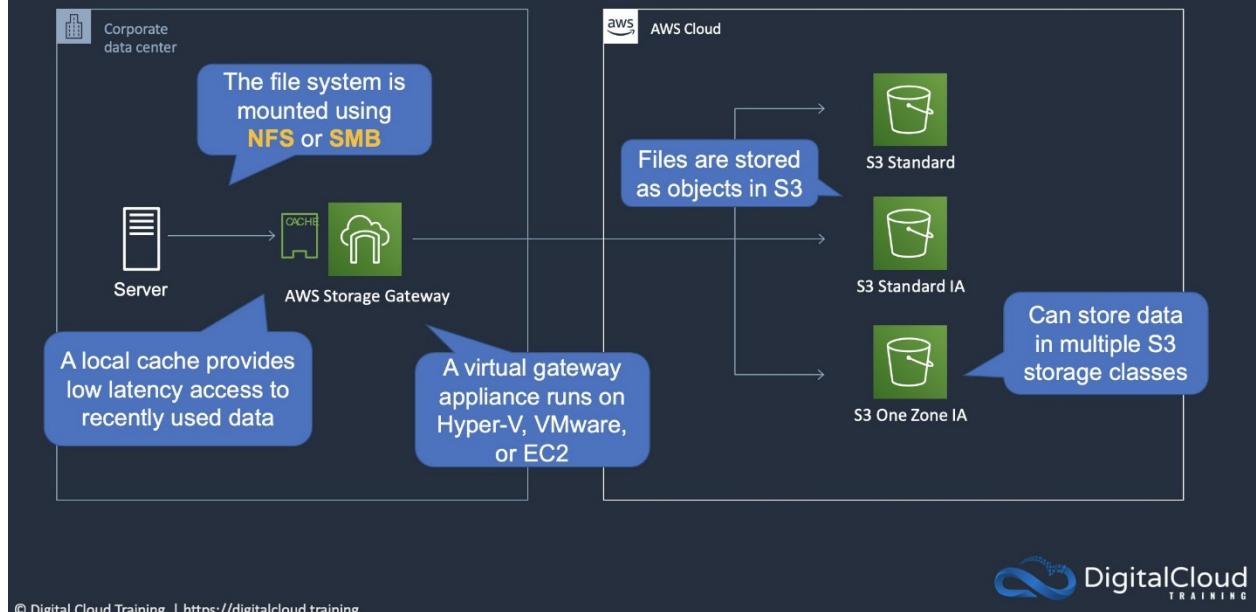
Answer: 4

Explanation:

The best solution for this requirement is to use an AWS Storage Gateway file gateway. This will provide a local NFS mount point for the data and a local cache. The data is then replicated to Amazon S3 where it can be analyzed by the Amazon EC2 instances in the AWS Cloud.



AWS Storage Gateway – File Gateway



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Use an AWS Storage Gateway file gateway to provide a locally accessible file system that replicates data to the cloud, then analyze the data in the AWS Cloud" is the correct answer.

INCORRECT: "Use an AWS Storage Gateway tape gateway to take a backup of the local data and store it on AWS, then perform analytics on this data in the AWS Cloud" is incorrect. A tape gateway does not provide a local NFS mount point, it is simply a backup solution not a file system.

INCORRECT: "Use an AWS Storage Gateway volume gateway in stored mode to regularly take snapshots of the local data, then copy the data to AWS" is incorrect. Volume gateways use block-based protocols not NFS.

INCORRECT: "Use an AWS Storage Gateway volume gateway in cached mode to back up all the local storage in the AWS Cloud, then perform analytics on this data in the cloud" is incorrect. Volume gateways use block-based protocols not NFS.

References:

<https://aws.amazon.com/storagegateway/file/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 45

A company has created an application that stores sales performance data in an Amazon DynamoDB table. A web application is being created to display the data. A Solutions Architect must design the web application using managed services that require minimal operational maintenance.

Which architectures meet these requirements? (Select TWO.)

1. An Amazon API Gateway REST API directly accesses the sales performance data in the DynamoDB table.
2. An Elastic Load Balancer forwards requests to a target group with the DynamoDB table configured as the target.
3. An Amazon API Gateway REST API invokes an AWS Lambda function. The Lambda function reads data from the DynamoDB table.
4. An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that reads data from the DynamoDB table.
5. An Amazon Route 53 hosted zone routes requests to an AWS Lambda endpoint to invoke a Lambda function that reads data from the DynamoDB table.

Answer: 1,3

Explanation:

There are two architectures here that fulfill the requirement to create a web application that displays the data from the DynamoDB table.

The first one is to use an API Gateway REST API that invokes an AWS Lambda function. A Lambda proxy integration can be used, and this will proxy the API requests to the Lambda function which processes the request and accesses the DynamoDB table.

The second option is to use an API Gateway REST API to directly access the sales performance data. In this case a proxy for the DynamoDB query API can be created using a method in the REST API.

CORRECT: "An Amazon API Gateway REST API invokes an AWS Lambda function. The Lambda function reads data from the DynamoDB table" is a correct answer.

CORRECT: "An Amazon API Gateway REST API directly accesses the sales performance data in the DynamoDB table" is also a correct answer.

INCORRECT: "An Amazon Route 53 hosted zone routes requests to an AWS Lambda endpoint to invoke a Lambda function that reads data from the DynamoDB table" is incorrect. An Alias record could be created in a hosted zone but a hosted zone itself does not route to a Lambda endpoint. Using an Alias, it is possible to route to a VPC endpoint that uses a Lambda function however there would not be a web front end so a REST API would be preferable.

INCORRECT: "An Elastic Load Balancer forwards requests to a target group with the DynamoDB table configured as the target" is incorrect. You cannot configure DynamoDB as a target in a target group.

INCORRECT: "An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that reads data from the DynamoDB table" is incorrect. This would not offer low operational maintenance as you must manage the EC2 instances.

References:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-create-api-as-simple-proxy-for-lambda.html>

<https://aws.amazon.com/blogs/compute/using-amazon-api-gateway-as-a-proxy-for-dynamodb/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

QUESTION 46

A company runs a business-critical application in the us-east-1 Region. The application uses an Amazon Aurora MySQL database cluster which is 2 TB in size. A Solutions Architect needs to determine a disaster recovery strategy for failover to the us-west-2 Region. The strategy must provide a recovery time objective (RTO) of 10 minutes and a recovery point objective (RPO) of 5 minutes.

Which strategy will meet these requirements?

1. 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.
2. 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. Use an Amazon EventBridge rule that invokes an AWS Lambda function to promote the DB cluster in us-west-2 when failure is detected.
3. Create a cross-Region Aurora MySQL read replica in us-west-2 Region. Configure an Amazon EventBridge rule that invokes an AWS Lambda function that promotes the read replica in us-west-2 when failure is detected.
4. Recreate the database as an Aurora multi master cluster across the us-east-1 and us-west-2 Regions with multiple writers to allow read/write capabilities from all database instances.

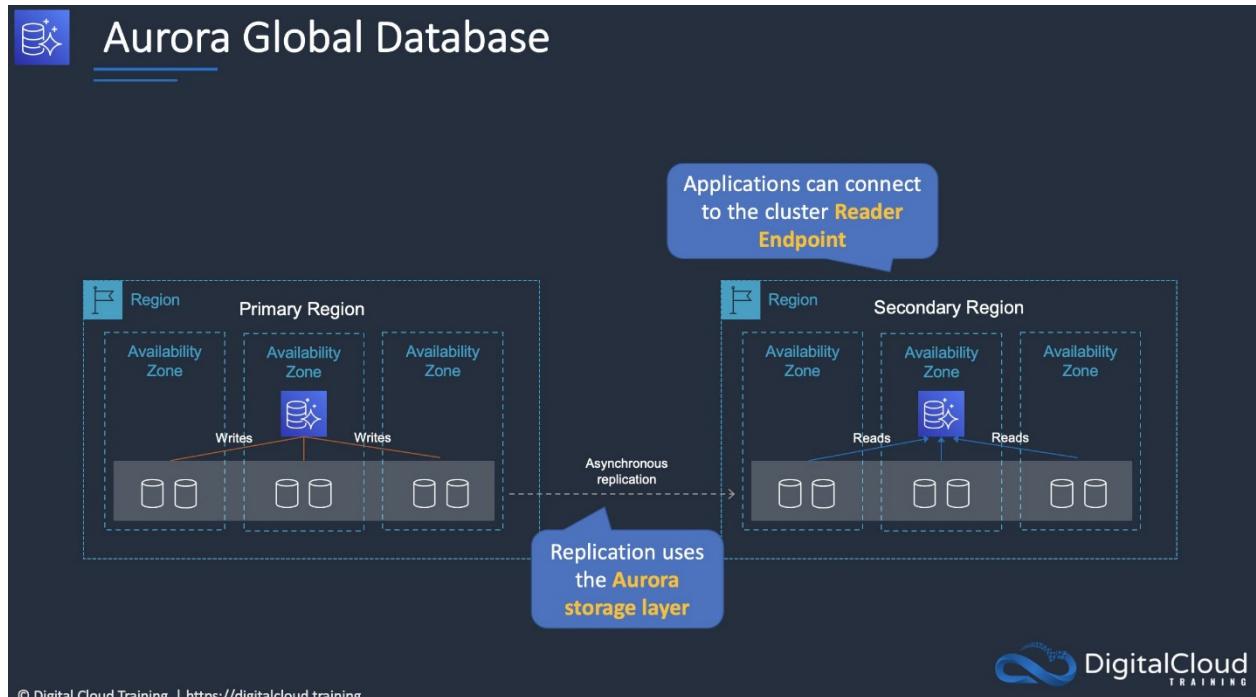
Answer: 2

Explanation:

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages

If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage.

This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "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. Use an Amazon EventBridge rule that invokes an AWS Lambda function to promote the DB cluster in us-west-2 when failure is detected" is the correct answer.

INCORRECT: "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" is incorrect. You cannot create a multi-Region Aurora MySQL DB cluster. Options are to create MySQL Replicas (may meet the RTO objectives), or to use global database.

INCORRECT: "Create a cross-Region Aurora MySQL read replica in us-west-2 Region. Configure an Amazon EventBridge rule that invokes an AWS Lambda function that promotes the read replica in us-west-2 when failure is detected" is incorrect. This may not meet the RTO objectives as large databases may well take more than 10 minutes to promote.

INCORRECT: "Recreate the database as an Aurora multi master cluster across the us-east-1 and us-west-2 Regions with multiple writers to allow read/write capabilities from all database instances" is incorrect. Multi master only works within a Region it does not work across Regions.

References:

<https://aws.amazon.com/rds/aurora/global-database/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>

QUESTION 47

An application runs on a fleet of Amazon EC2 instances in an Amazon EC2 Auto Scaling group behind an Elastic Load Balancer. The operations team has determined that the application performs best when the CPU utilization of the EC2 instances is at or near 60%.

Which scaling configuration should a Solutions Architect use to optimize the applications performance?

1. Use a simple scaling policy to dynamically scale the Auto Scaling group.

2. Use a step scaling policy to dynamically scale the Auto Scaling group.
3. Use a scheduled scaling policy to dynamically scale the Auto Scaling group.
4. Use a target tracking policy to dynamically scale the Auto Scaling group.

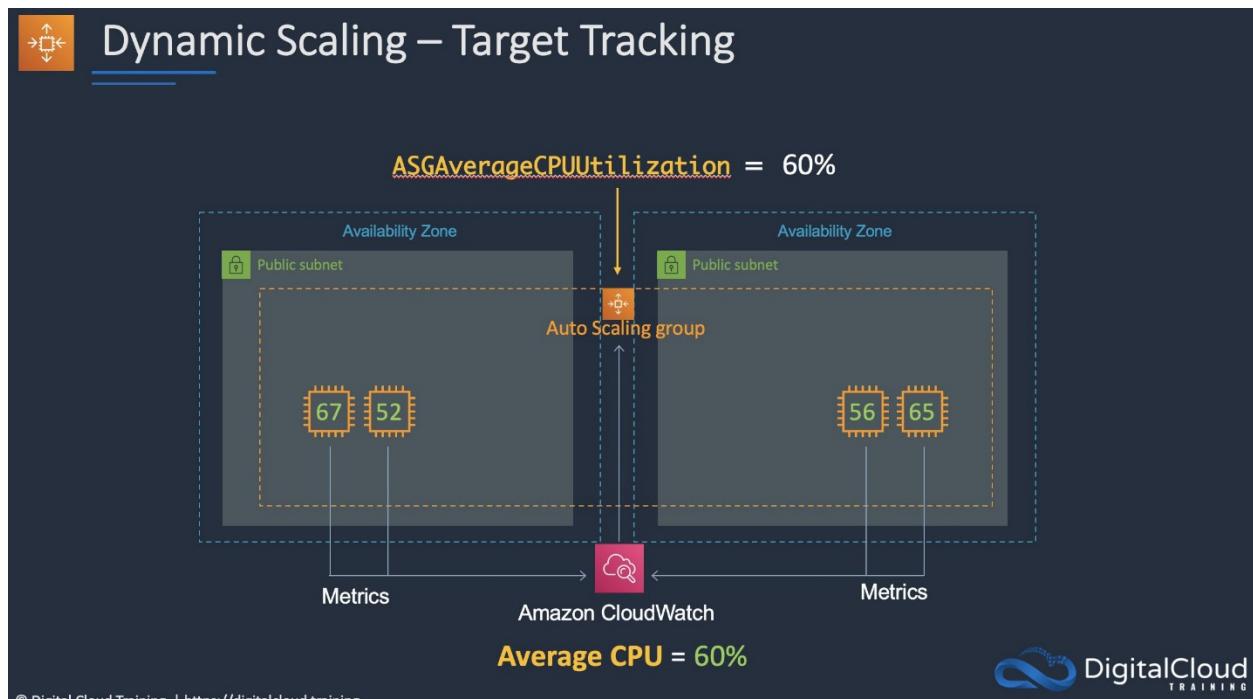
Answer: 4

Explanation:

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value.

The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern.

The following diagram shows a target tracking policy set to keep the CPU utilization of the EC2 instances at or close to 60%.



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Use a target tracking policy to dynamically scale the Auto Scaling group" is the correct answer.

INCORRECT: "Use a simple scaling policy to dynamically scale the Auto Scaling group" is incorrect. Simple scaling is not used for maintaining a target utilization. It is used for making simple adjustments up or down based on a threshold value.

INCORRECT: "Use a step scaling policy to dynamically scale the Auto Scaling group" is incorrect. Step scaling is not used for maintaining a target utilization. It is used for making step adjustments that vary based on the size of the alarm breach.

INCORRECT: "Use a scheduled scaling policy to dynamically scale the Auto Scaling group" is incorrect. Scheduled scaling is not used for maintaining a target utilization. It is used for scheduling changes at specific dates and times.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 48

A company's staff connect from home office locations to administer applications using bastion hosts in a single AWS Region.

The company requires a resilient bastion host architecture that requires minimal ongoing operational overhead.

How can a Solutions Architect best meet these requirements?

1. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones.
2. Create a Network Load Balancer backed by Reserved Instances in a cluster placement group.
3. Create a Network Load Balancer backed by the existing servers in different Availability Zones.
4. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple AWS Regions.

Answer: 1

Explanation:

Bastion hosts (aka “jump hosts”) are EC2 instances in public subnets that administrators and operations staff can connect to from the internet. From the bastion host they are then able to connect to other instances and applications within AWS by using internal routing within the VPC.

All answers use a Network Load Balancer which is acceptable for forwarding incoming connections to targets. The differences are in where the connections are forwarded to. The best option is to create an Auto Scaling group with EC2 instances in multiple Availability Zones. This creates a resilient architecture within a single AWS Region which is exactly what the question asks for.

CORRECT: "Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones" is the correct answer.

INCORRECT: "Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple AWS Regions" is incorrect. You cannot have instances in an ASG across multiple Regions and you can't have an NLB distribute connections across multiple Regions.

INCORRECT: "Create a Network Load Balancer backed by Reserved Instances in a cluster placement group" is incorrect. A cluster placement group packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly coupled node-to-node communication that is typical of HPC applications.

INCORRECT: "Create a Network Load Balancer backed by the existing servers in different Availability Zones" is incorrect. An Auto Scaling group is required to maintain instances in different AZs for resilience.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 49

A Solutions Architect has been tasked with migrating 30 TB of data from an on-premises data center within 20 days. The company has an internet connection that is limited to 25 Mbps and the data transfer cannot use more than 50% of the connection speed.

What should a Solutions Architect do to meet these requirements?

1. Use AWS DataSync.
2. Use AWS Storage Gateway.
3. Use AWS Snowball.
4. Use a site-to-site VPN.

Answer: 3

Explanation:

This is a simple case of working out roughly how long it will take to migrate the data using the 12.5 Mbps of bandwidth that is available for transfer and seeing which options are feasible. Transferring 30 TB of data across a 25 Mbps connection could take upwards of 200 days.

Therefore, we know that using the Internet connection will not meet the requirements and we can rule out any solution that will use the internet (all options except for Snowball). AWS Snowball is a physical device that is shipped to your office or data center. You can then load data onto it and ship it back to AWS where the data is uploaded to Amazon S3.

Snowball is the only solution that will achieve the data migration requirements within the 20-day period.

CORRECT: "Use AWS Snowball" is the correct answer.

INCORRECT: "Use AWS DataSync" is incorrect. This uses the internet which will not meet the 20-day deadline.

INCORRECT: "Use AWS Storage Gateway" is incorrect. This uses the internet which will not meet the 20-day deadline.

INCORRECT: "Use a site-to-site VPN" is incorrect. This uses the internet which will not meet the 20-day deadline.

References:

<https://aws.amazon.com/snowball/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 50

A company runs a containerized application on an Amazon Elastic Kubernetes Service (EKS) using a microservices architecture. The company requires a solution to collect, aggregate, and summarize metrics and logs. The solution should provide a centralized dashboard for viewing information including CPU and memory utilization for EKS namespaces, services, and pods.

Which solution meets these requirements?

1. Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
2. Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
3. Migrate the containers to Amazon ECS and enable Amazon CloudWatch Container Insights. View the metrics and logs in the CloudWatch console.
4. Configure AWS X-Ray to enable tracing for the EKS microservices. Query the trace data using Amazon Elasticsearch.

Answer: 1

Explanation:

Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. Container Insights is available for Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and Kubernetes platforms on Amazon EC2.

With Container Insights for EKS you can see the top contributors by memory or CPU, or the most recently active resources. This is available when you select any of the following dashboards in the drop-down box near the top of the page:

- ECS Services
- ECS Tasks
- EKS Namespaces
- EKS Services
- EKS Pods

CORRECT: "Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console" is the correct answer.

INCORRECT: "Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console" is incorrect. Container Insights is the best way to view the required data.

INCORRECT: "Migrate the containers to Amazon ECS and enable Amazon CloudWatch Container Insights. View the metrics and logs in the CloudWatch console" is incorrect. There is no need to migrate containers to ECS as EKS is supported for Container Insights.

INCORRECT: "Configure AWS X-Ray to enable tracing for the EKS microservices. Query the trace data using Amazon Elasticsearch" is incorrect. X-Ray will not deliver the required statistics to a centralized dashboard.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContainerInsights.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

QUESTION 51

A company is deploying a solution for sharing media files around the world using Amazon CloudFront with an Amazon S3 origin configured as a static website. The company requires that all traffic for the website must be inspected by AWS WAF.

Which solution meets these requirements?

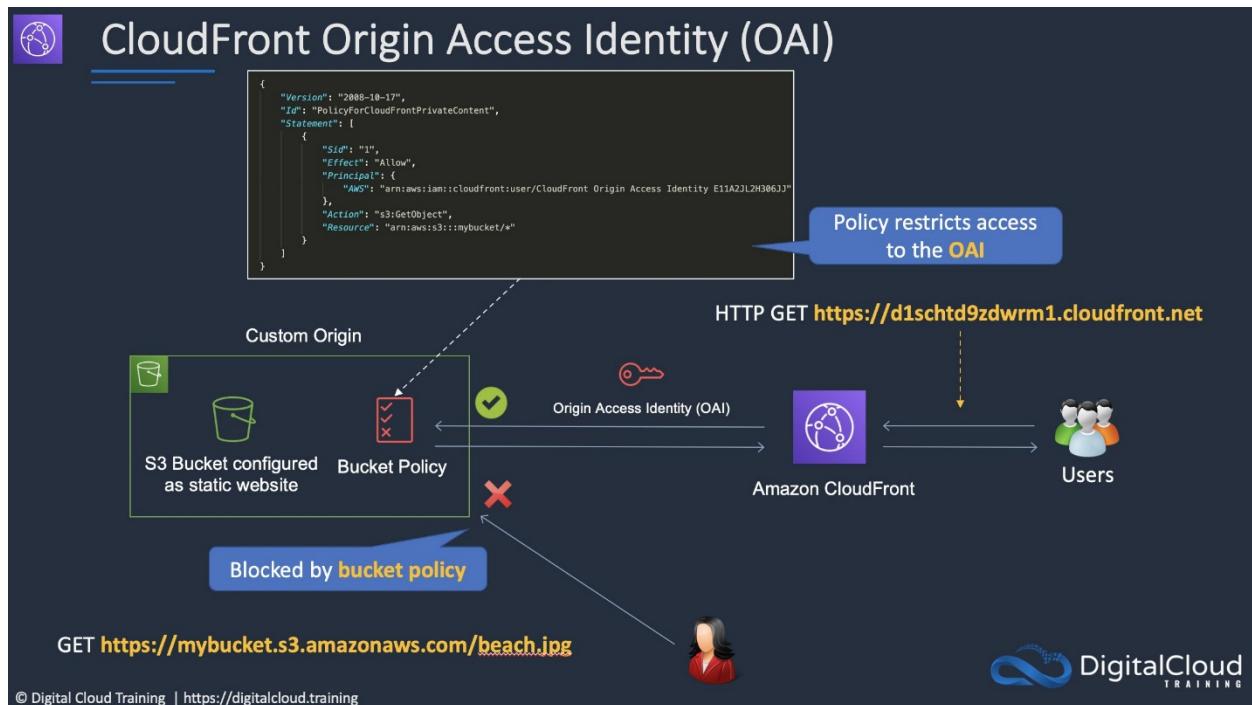
1. Deploy CloudFront with an S3 origin and configure an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the CloudFront distribution.
2. Create a Network ACL that limits access to the S3 bucket to the CloudFront IP addresses. Attach a WebACL to the CloudFront distribution.
3. Use an Amazon Route 53 Alias record to forward traffic for the website to AWS WAF. Configure AWS WAF to inspect traffic and attach the CloudFront distribution.
4. Create an S3 bucket policy with a condition that only allows requests that originate from AWS WAF.

Answer: 1

Explanation:

The AWS Web Application Firewall (WAF) can be attached to an Amazon CloudFront distribution to enable protection from web exploits. In this case the distribution uses an S3 origin, and the question is stating that all traffic must be inspected by AWS WAF. This means we need to ensure that requests cannot circumvent AWS WAF and hit the S3 bucket directly.

This can be achieved by configuring an origin access identity (OAI) which is a special type of CloudFront user that is created within the distribution and configured in an S3 bucket policy. The policy will only allow requests that come from the OAI which means all requests must come via the distribution and cannot hit S3 directly.



CORRECT: "Deploy CloudFront with an S3 origin and configure an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the CloudFront distribution" is the correct answer.

INCORRECT: "Create a Network ACL that limits access to the S3 bucket to the CloudFront IP addresses. Attach a WebACL to the CloudFront distribution" is incorrect. Network ACLs restrict traffic in/out of subnets but S3 is a public service.

INCORRECT: "Use an Amazon Route 53 Alias record to forward traffic for the website to AWS WAF. Configure AWS WAF to inspect traffic and attach the CloudFront distribution" is incorrect. You cannot direct traffic to AWS WAF using an Alias record.

INCORRECT: "Create an S3 bucket policy with a condition that only allows requests that originate from AWS WAF" is incorrect. This cannot be done. Instead use an OAI in the bucket policy.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 52

A company has created a disaster recovery solution for an application that runs behind an Application Load Balancer (ALB). The DR solution consists of a second copy of the application running behind a second ALB in another Region. The Solutions Architect requires a method of automatically updating the DNS record to point to the ALB in the second Region.

What action should the Solutions Architect take?

1. Enable an ALB health check.
2. Use Amazon EventBridge to cluster the ALBs.
3. Enable an Amazon Route 53 health check.
4. Configure an alarm on a CloudTrail trail.

Answer: 3

Explanation:

Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. Each health check that you create can monitor one of the following:

- The health of a specified resource, such as a web server
- The status of other health checks
- The status of an Amazon CloudWatch alarm

Health checks can be used with other configurations such as a failover routing policy. In this case a failover routing policy will direct traffic to the ALB of the primary Region unless health checks fail at which time it will direct traffic to the secondary record for the DR ALB.

CORRECT: "Enable an Amazon Route 53 health check" is the correct answer.

INCORRECT: "Enable an ALB health check" is incorrect. This will simply perform health checks of the instances behind the ALB, rather than the ALB itself. This could be used in combination with Route 53 health checks.

INCORRECT: "Use Amazon EventBridge to cluster the ALBs" is incorrect. You cannot cluster ALBs in any way.

INCORRECT: "Configure an alarm on a CloudTrail trail" is incorrect. CloudTrail records API activity so this does not help.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

QUESTION 53

A company has deployed an application that consists of several microservices running on Amazon EC2 instances behind an Amazon API Gateway API. A Solutions Architect is concerned that the microservices are not designed to elastically scale when large increases in demand occur.

Which solution addresses this concern?

1. Create an Amazon SQS queue to store incoming requests. Configure the microservices to retrieve the requests from the queue for processing.
2. Use Amazon CloudWatch alarms to notify operations staff when the microservices are suffering high CPU utilization.
3. Spread the microservices across multiple Availability Zones and configure Amazon Data Lifecycle Manager to take regular snapshots.

4. Use an Elastic Load Balancer to distribute the traffic between the microservices. Configure Amazon CloudWatch metrics to monitor traffic to the microservices.

Answer: 1

Explanation:

The individual microservices are not designed to scale. Therefore, the best way to ensure they are not overwhelmed by requests is to decouple the requests from the microservices. An Amazon SQS queue can be created, and the API Gateway can be configured to add incoming requests to the queue. The microservices can then pick up the requests from the queue when they are ready to process them.

CORRECT: "Create an Amazon SQS queue to store incoming requests. Configure the microservices to retrieve the requests from the queue for processing" is the correct answer.

INCORRECT: "Use Amazon CloudWatch alarms to notify operations staff when the microservices are suffering high CPU utilization" is incorrect. This solution requires manual intervention and does not help the application to elastically scale.

INCORRECT: "Spread the microservices across multiple Availability Zones and configure Amazon Data Lifecycle Manager to take regular snapshots" is incorrect. This does not automate the elasticity of the application.

INCORRECT: "Use an Elastic Load Balancer to distribute the traffic between the microservices. Configure Amazon CloudWatch metrics to monitor traffic to the microservices" is incorrect. You cannot use an ELB spread traffic across many different individual microservices as the requests must be directed to individual microservices. Therefore, you would need a target group per microservice, and you would need Auto Scaling to scale the microservices.

References:

<https://aws.amazon.com/blogs/compute/understanding-asynchronous-messaging-for-microservices/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 54

A Solutions Architect is designing a solution for an application that requires very low latency between the client and the backend. The application uses the UDP protocol, and the backend is hosted on Amazon EC2 instances. The solution must be highly available across multiple Regions and users around the world should be directed to the most appropriate Region based on performance.

How can the Solutions Architect meet these requirements?

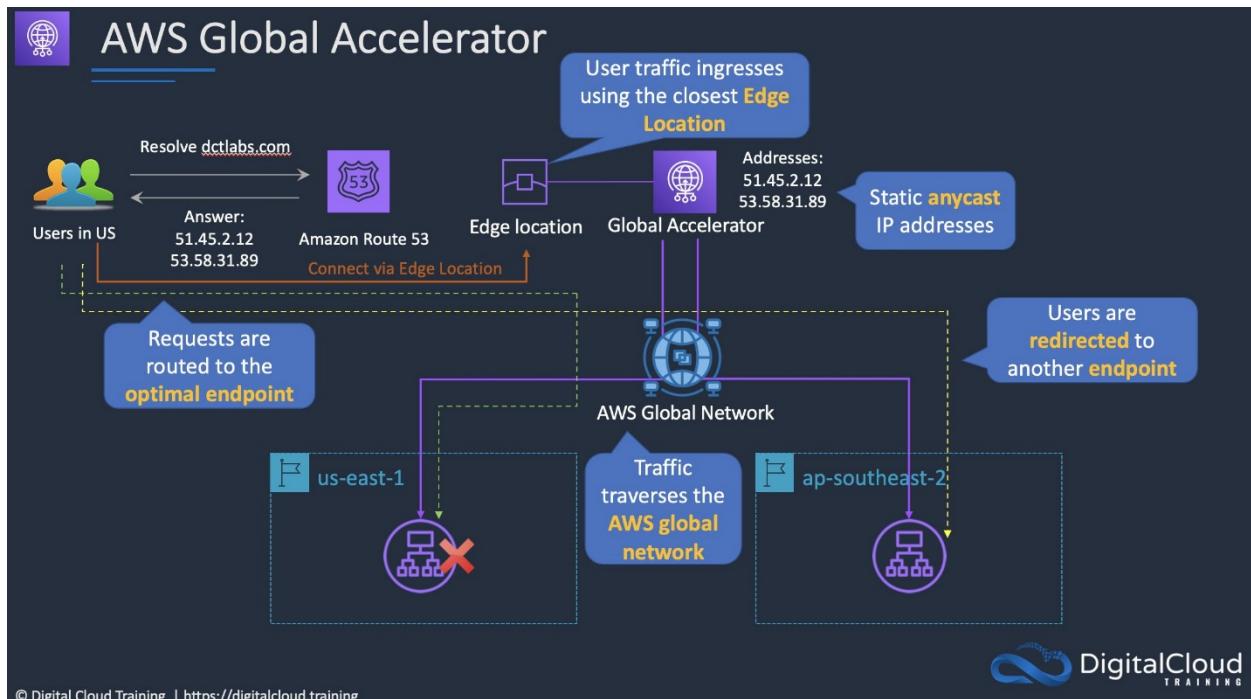
1. Deploy Amazon EC2 instances in multiple Regions. Create a multivalue answer routing record in Amazon Route 53 that includes all EC2 endpoints.
2. Deploy an Application Load Balancer in front of the EC2 instances in each Region. Use AWS WAF to direct traffic to the most optimal Regional endpoint.
3. Deploy an Amazon CloudFront distribution with a custom origin pointing to Amazon EC2 instances in multiple Regions.
4. Deploy a Network Load Balancer in front of the EC2 instances in each Region. Use AWS Global Accelerator to route traffic to the most optimal Regional endpoint.

Answer: 4

Explanation:

An NLB is ideal for latency-sensitive applications and can listen on UDP for incoming requests. As Elastic Load Balancers are region-specific it is necessary to have an NLB in each Region in front of the EC2 instances.

To direct traffic based on optimal performance, AWS Global Accelerator can be used. GA will ensure traffic is routed across the AWS global network to the most optimal endpoint based on performance.



© Digital Cloud Training | <https://digitalcloud.training>



CORRECT: "Deploy a Network Load Balancer in front of the EC2 instances in each Region. Use AWS Global Accelerator to route traffic to the most optimal Regional endpoint" is the correct answer.

INCORRECT: "Deploy an Application Load Balancer in front of the EC2 instances in each Region. Use AWS WAF to direct traffic to the most optimal Regional endpoint" is incorrect. You cannot use WAF to direct traffic to endpoints based on performance.

INCORRECT: "Deploy an Amazon CloudFront distribution with a custom origin pointing to Amazon EC2 instances in multiple Regions" is incorrect. CloudFront cannot listen on UDP, it is used for HTTP/HTTPS.

INCORRECT: "Deploy Amazon EC2 instances in multiple Regions. Create a multivalue answer routing record in Amazon Route 53 that includes all EC2 endpoints" is incorrect. This configuration would not route incoming requests to the most optimal endpoint based on performance, it would provide multiple records in answers and traffic would be distributed across multiple Regions.

References:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-global-accelerator/>

QUESTION 55

An application has multiple components for receiving requests that must be processed and subsequently processing the requests. The company requires a solution for decoupling the application components. The application receives around 10,000 requests per day and requests can take up to 2 days to process. Requests that fail to process must be retained.

Which solution meets these requirements most efficiently?

1. Create an Amazon DynamoDB table and enable DynamoDB streams. Configure the processing component to process requests from the stream.
2. Decouple the application components with an Amazon SQS queue. Configure a dead-letter queue to collect the requests that failed to process.
3. Use an Amazon Kinesis data stream to decouple application components and integrate the processing component with the Kinesis Client Library (KCL).

4. Decouple the application components with an Amazon SQS Topic. Configure the receiving component to subscribe to the SNS Topic.

Answer: 2

Explanation:

The Amazon Simple Queue Service (SQS) is ideal for decoupling the application components. Standard queues can support up to 120,000 in flight messages and messages can be retained for up to 14 days in the queue.

To ensure the retention of requests (messages) that fail to process, a dead-letter queue can be configured. Messages that fail to process are sent to the dead-letter queue (based on the redrive policy) and can be subsequently dealt with.

CORRECT: "Decouple the application components with an Amazon SQS queue. Configure a dead-letter queue to collect the requests that failed to process" is the correct answer.

INCORRECT: "Decouple the application components with an Amazon SQS Topic. Configure the receiving component to subscribe to the SNS Topic" is incorrect. SNS does not store requests, it immediately forwards all notifications to subscribers.

INCORRECT: "Use an Amazon Kinesis data stream to decouple application components and integrate the processing component with the Kinesis Client Library (KCL)" is incorrect. This is a less efficient solution and will likely be less cost-effective compared to using Amazon SQS. There is also no option for retention of requests that fail to process.

INCORRECT: "Create an Amazon DynamoDB table and enable DynamoDB streams. Configure the processing component to process requests from the stream" is incorrect. This solution does not offer any way of retaining requests that fail to process or removal of items from the table and is therefore less efficient.

References:

<https://aws.amazon.com/sqs/faqs/>

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

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 56

A Solutions Architect created the following policy and associated to an AWS IAM group containing several administrative users:
{

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:TerminateInstances",
        "Resource": "*",
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": "10.1.2.0/24"
            }
        }
    },
    {
        "Effect": "Deny",
        "Action": "ec2:*",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {

```

```

        "ec2:Region": "us-east-1"
    }
}
]
}

```

What is the effect of this policy?

1. Administrators can terminate an EC2 instance in any AWS Region except us-east-1.
2. Administrators can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28.
3. Administrators can terminate an EC2 instance with the IP address 10.1.2.5 in the us-east-1 Region.
4. Administrators cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28.

Answer: 2

Explanation:

The Condition element (or Condition *block*) lets you specify conditions for when a policy is in effect. The Condition element is optional. In the Condition element, you build expressions in which you use condition operators (equal, less than, etc.) to match the condition keys and values in the policy against keys and values in the request context.

In this policy statement the first block allows the "ec2:TerminateInstances" API action only if the IP address of the requester is within the "10.1.2.0/24" range. This is specified using the "aws:SourceIp" condition.

The second block denies all EC2 API actions with a conditional operator (StringNotEquals) that checks the Region the request is being made in ("ec2:Region"). If the Region is any value other than us-east-1 the request will be denied. If the Region the request is being made in is us-east-1 the request will not be denied.

CORRECT: "Administrators can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28" is the correct answer.

INCORRECT: "Administrators cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28" is incorrect. This is not true; the conditions allow this action.

INCORRECT: "Administrators can terminate an EC2 instance in any AWS Region except us-east-1" is incorrect. The API action to terminate instances only has a condition of the source IP. If the source IP is in the range it will allow. The second block only denies API actions if the Region is NOT us-east-1. Therefore, the user can terminate instances in us-east-1

INCORRECT: "Administrators can terminate an EC2 instance with the IP address 10.1.2.5 in the us-east-1 Region" is incorrect. The aws:SourceIp condition is checking the IP address of the requester (where you're making the call from), not the resource you want to terminate.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 57

A company has several AWS accounts that are used by developers for development, testing and pre-production environments. The company has received large bills for Amazon EC2 instances that are underutilized. A Solutions Architect has been tasked with restricting the ability to launch large EC2 instances in all accounts.

How can the Solutions Architect meet this requirement with the LEAST operational overhead?

1. Create a service-linked role for Amazon EC2 and attach a policy that denies the launch of large EC2 instances.
2. Create a resource-based policy that denies the launch of large EC2 instances and attach it to Amazon EC2 in each account.
3. Create an organization in AWS Organizations that includes all accounts and create a service control policy (SCP) that denies the launch of large EC2 instances.
4. Create an IAM role in each account that denies the launch of large EC2 instances. Grant the developers IAM group access to the role.

Answer: 3**Explanation:**

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to the IAM users and roles in the affected accounts.

In this case the Solutions Architect can use an SCP to define a restriction that denies the launch of large EC2 instances. The SCP can be applied to all accounts, and this will ensure that even those users with permissions to launch EC2 instances will be restricted to smaller EC2 instance types.

CORRECT: "Create an organization in AWS Organizations that includes all accounts and create a service control policy (SCP) that denies the launch of large EC2 instances" is the correct answer.

INCORRECT: "Create a service-linked role for Amazon EC2 and attach a policy that denies the launch of large EC2 instances" is incorrect. You cannot create service-linked roles yourself; they are created by AWS with predefined policies.

INCORRECT: "Create a resource-based policy that denies the launch of large EC2 instances and attach it to Amazon EC2 in each account" is incorrect. You cannot attach a resource-based policy to Amazon EC2.

INCORRECT: "Create an IAM role in each account that denies the launch of large EC2 instances. Grant the developers IAM group access to the role" is incorrect. This is much less operationally efficient compared to using SCPs with AWS Organizations.

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-organizations/>

QUESTION 58

A Solutions Architect is designing an application that will run on Amazon EC2 instances. The application will use Amazon S3 for storing image files and an Amazon DynamoDB table for storing customer information. The security team require that traffic between the EC2 instances and AWS services must not traverse the public internet.

How can the Solutions Architect meet the security team's requirements?

1. Create gateway VPC endpoints for Amazon S3 and DynamoDB.
2. Create a NAT gateway in a public subnet and configure route tables.
3. Create interface VPC endpoints for Amazon S3 and DynamoDB.
4. Create a virtual private gateway and configure VPC route tables.

Answer: 1**Explanation:**

A VPC endpoint enables private connections between your VPC and supported AWS services and VPC endpoint services powered by AWS PrivateLink. A gateway endpoint is used for Amazon S3 and Amazon DynamoDB. You specify a gateway endpoint as a route table target for traffic that is destined for the supported AWS services.

CORRECT: "Create gateway VPC endpoints for Amazon S3 and DynamoDB" is the correct answer.

INCORRECT: "Create a NAT gateway in a public subnet and configure route tables" is incorrect. A NAT gateway is used for enabling internet connectivity for instances in private subnets. Connections will traverse the internet.

INCORRECT: "Create interface VPC endpoints for Amazon S3 and DynamoDB" is incorrect. You should use a gateway VPC endpoint for S3 and DynamoDB.

INCORRECT: "Create a virtual private gateway and configure VPC route tables" is incorrect. VGWs are used for VPN connections, they do not allow access to AWS services from a VPC.

References:

<https://docs.aws.amazon.com/vpc/latestprivatelink/vpc-endpoints.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon->

QUESTION 59

A Solutions Architect needs a solution for hosting a website that will be used by a development team. The website contents will consist of HTML, CSS, client-side JavaScript, and images.

Which solution is MOST cost-effective?

1. Launch an Amazon EC2 instance and host the website there.
2. Use a Docker container to host the website on AWS Fargate.
3. Create an Application Load Balancer with an AWS Lambda target.
4. Create an Amazon S3 bucket and host the website there.

Answer: 4

Explanation:

Amazon S3 can be used for hosting static websites and cannot be used for dynamic content. In this case the content is purely static with client-side code running. Therefore, an S3 static website will be the most cost-effective solution for hosting this website.

CORRECT: "Create an Amazon S3 bucket and host the website there" is the correct answer.

INCORRECT: "Launch an Amazon EC2 instance and host the website there" is incorrect. This will be more expensive as it uses an EC2 instances.

INCORRECT: "Use a Docker container to host the website on AWS Fargate" is incorrect. A static website on S3 is sufficient for this use case and will be more cost-effective than Fargate.

INCORRECT: "Create an Application Load Balancer with an AWS Lambda target" is incorrect. This is also a more expensive solution and unnecessary for this use case.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 60

An application runs on Amazon EC2 instances in a private subnet. The EC2 instances process data that is stored in an Amazon S3 bucket. The data is highly confidential and a private and secure connection is required between the EC2 instances and the S3 bucket.

Which solution meets these requirements?

1. Configure encryption for the S3 bucket using an AWS KMS key.
2. Configure a custom SSL/TLS certificate on the S3 bucket.
3. Set up S3 bucket policies to allow access from a VPC endpoint.
4. Set up an IAM policy to grant read-write access to the S3 bucket.

Answer: 3

Explanation:

A gateway VPC endpoint can be used to access an Amazon S3 bucket using private IP addresses. To further secure the solution an S3 bucket policy can be created that restricts access to the VPC endpoint so connections cannot be made to the bucket from other sources.

CORRECT: "Set up S3 bucket policies to allow access from a VPC endpoint" is the correct answer.

INCORRECT: "Set up an IAM policy to grant read-write access to the S3 bucket" is incorrect. This does not enable private access from EC2. A gateway VPC endpoint is required.

INCORRECT: "Configure encryption for the S3 bucket using an AWS KMS key" is incorrect. This will encrypt data at rest but does not secure the connection to the bucket or ensure private connections must be made.

INCORRECT: "Configure a custom SSL/TLS certificate on the S3 bucket" is incorrect. You cannot add a custom SSL/TLS certificate

to Amazon S3.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 61

A systems administrator of a company wants to detect and remediate the compromise of services such as Amazon EC2 instances and Amazon S3 buckets.

Which AWS service can the administrator use to protect the company against attacks?

1. Amazon Cognito
2. Amazon Inspector
3. Amazon Macie
4. Amazon GuardDuty

Answer: 4

Explanation:

Amazon GuardDuty gives you access to built-in detection techniques that are developed and optimized for the cloud. The detection algorithms are maintained and continuously improved upon by AWS Security. The primary detection categories include reconnaissance, instance compromise, account compromise, and bucket compromise.

Amazon GuardDuty offers HTTPS APIs, CLI tools, and Amazon CloudWatch Events to support automated security responses to security findings. For example, you can automate the response workflow by using CloudWatch Events as an event source to trigger an AWS Lambda function.

CORRECT: "Amazon GuardDuty" is the correct answer.

INCORRECT: "Amazon Cognito" is incorrect. Cognito provides sign up and sign services for mobile apps.

INCORRECT: "Amazon Inspector" is incorrect. Inspector is more about identifying vulnerabilities and evaluating against security best practices. It does not detect compromise.

INCORRECT: "Amazon Macie" is incorrect. Macie is used for detecting and protecting sensitive data that is in Amazon S3.

References:

<https://aws.amazon.com/guardduty/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-certified-cloud-practitioner/additional-aws-services-tools/>

QUESTION 62

A company is creating a solution that must offer disaster recovery across multiple AWS Regions. The solution requires relational a database that can support a Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

1. Amazon RDS for with Multi-AZ enabled.
2. Amazon DynamoDB global tables.
3. Amazon Aurora Global Database.
4. Amazon RDS for with a cross-Region replica.

Answer: 3

Explanation:

Aurora Global Database lets you easily scale database reads across the world and place your applications close to your users. Your applications enjoy quick data access regardless of the number and location of secondary regions, with typical cross-region replication latencies below 1 second.

If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take

read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

CORRECT: "Amazon Aurora Global Database" is the correct answer.

INCORRECT: "Amazon RDS for with Multi-AZ enabled" is incorrect. RDS Multi-AZ is across availability zones, not across Regions.

INCORRECT: "Amazon RDS for with a cross-Region replica" is incorrect. A cross-Region replica for RDS cannot provide an RPO of 1 second as there is typically more latency. You also cannot achieve a minute RPO as it takes much longer to promote a replica to a master.

INCORRECT: "Amazon DynamoDB global tables" is incorrect. This is not a relational database; it is a non-relational database (NoSQL).

References:

<https://aws.amazon.com/rds/aurora/global-database/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-aurora/>

QUESTION 63

A company is deploying an analytics application on AWS Fargate. The application requires connected storage that offers concurrent access to files and high performance.

Which storage option should the solutions architect recommend?

1. Create an Amazon EFS file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
2. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
3. Create an Amazon EBS volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.
4. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.

Answer: 1

Explanation:

The Amazon Elastic File System offers concurrent access to a shared file system and provides high performance. You can create file system policies for controlling access and then use an IAM role that is specified in the policy for access.

CORRECT: "Create an Amazon EFS file share and establish an IAM role that allows Fargate to communicate with Amazon EFS" is the correct answer.

INCORRECT: "Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3" is incorrect. S3 uses a REST API not a file system API so access can be shared but is not concurrent.

INCORRECT: "Create an Amazon EBS volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS" is incorrect. EBS volumes cannot be shared amongst Fargate tasks, they are used with EC2 instances.

INCORRECT: "Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre" is incorrect. It is not supported to connect Fargate to FSx for Lustre.

References:

<https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 64

An application runs on Amazon EC2 instances backed by Amazon EBS volumes and an Amazon RDS database. The application is highly sensitive and security compliance requirements mandate that all personally identifiable information (PII) be encrypted at rest.

Which solution should a Solutions Architect choose to this requirement?

1. Enable encryption on Amazon RDS during creation. Use Amazon Macie to identify sensitive data.
2. Configure Amazon EBS encryption and Amazon RDS encryption with AWS KMS keys to encrypt instance and database volumes.
3. Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes.
4. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.

Answer: 2

Explanation:

The data must be encrypted at rest on both the EC2 instance's attached EBS volumes and the RDS database. Both storage locations can be encrypted using AWS KMS keys. With RDS, KMS uses a customer master key (CMK) to encrypt the DB instance, all logs, backups, and snapshots.

CORRECT: "Configure Amazon EBS encryption and Amazon RDS encryption with AWS KMS keys to encrypt instance and database volumes" is the correct answer.

INCORRECT: "Enable encryption on Amazon RDS during creation. Use Amazon Macie to identify sensitive data" is incorrect. This does not encrypt the EBS volumes attached to the EC2 instance and Macie cannot be used with RDS.

INCORRECT: "Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes" is incorrect. SSL encryption encrypts data in transit but not at rest.

INCORRECT: "Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes" is incorrect. CloudHSM is not required for this solution, and we need to encrypt the database volumes and the EBS volumes.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 65

An application generates unique files that are returned to customers after they submit requests to the application. The application uses an Amazon CloudFront distribution for sending the files to customers. The company wishes to reduce data transfer costs without modifying the application.

How can this be accomplished?

1. Enable caching on the CloudFront distribution to store generated files at the edge.
2. Use AWS Global Accelerator to reduce application latency for customers.
3. Enable Amazon S3 Transfer Acceleration to reduce the transfer times.
4. Use Lambda@Edge to compress the files as they are sent to users.

Answer: 4

Explanation:

Lambda@Edge is a feature of Amazon CloudFront that lets you run code closer to users of your application, which improves performance and reduces latency. Lambda@Edge runs code in response to events generated by the Amazon CloudFront.

You simply upload your code to AWS Lambda, and it takes care of everything required to run and scale your code with high availability at an AWS location closest to your end user.

In this case Lambda@Edge can compress the files before they are sent to users which will reduce data egress costs.

CORRECT: "Use Lambda@Edge to compress the files as they are sent to users" is the correct answer.

INCORRECT: "Enable caching on the CloudFront distribution to store generated files at the edge" is incorrect. The files are unique to each customer request, so caching does not help.

INCORRECT: "Use AWS Global Accelerator to reduce application latency for customers" is incorrect. The aim is to reduce cost not latency and AWS GA uses the same network as CloudFront so does not assist with latency anyway.

INCORRECT: "Enable Amazon S3 Transfer Acceleration to reduce the transfer times" is incorrect. This does not lower costs.

References:

<https://aws.amazon.com/lambda/edge/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

SET 4: PRACTICE QUESTIONS ONLY

For training purposes, go directly to [Set 4: Practice Questions, Answers & Explanations](#)

QUESTION 1

A company is deploying an Amazon ElastiCache for Redis cluster. To enhance security a password should be required to access the database. What should the solutions architect use?

1. AWS Directory Service
2. AWS IAM Policy
3. Redis AUTH command
4. VPC Security Group

QUESTION 2

To increase performance and redundancy for an application a company has decided to run multiple implementations in different AWS Regions behind network load balancers. The company currently advertise the application using two public IP addresses from separate /24 address ranges and would prefer not to change these. Users should be directed to the closest available application endpoint.

Which actions should a solutions architect take? (Select TWO.)

1. Create an Amazon Route 53 geolocation based routing policy
2. Create an AWS Global Accelerator and attach endpoints in each AWS Region
3. Assign new static anycast IP addresses and modify any existing pointers
4. Migrate both public IP addresses to the AWS Global Accelerator
5. Create PTR records to map existing public IP addresses to an Alias

QUESTION 3

Three Amazon VPCs are used by a company in the same region. The company has two AWS Direct Connect connections to two separate company offices and wishes to share these with all three VPCs. A Solutions Architect has created an AWS Direct Connect gateway. How can the required connectivity be configured?

1. Associate the Direct Connect gateway to a transit gateway
2. Associate the Direct Connect gateway to a virtual private gateway in each VPC
3. Create a VPC peering connection between the VPCs and route entries for the Direct Connect Gateway
4. Create a transit virtual interface between the Direct Connect gateway and each VPC

QUESTION 4

A retail organization sends coupons out twice a week and this results in a predictable surge in sales traffic. The application runs on Amazon EC2 instances behind an Elastic Load Balancer. The organization is looking for ways lower costs while ensuring they meet the demands of their customers.

How can they achieve this goal?

1. Use capacity reservations with savings plans
2. Use a mixture of spot instances and on demand instances
3. Increase the instance size of the existing EC2 instances
4. Purchase Amazon EC2 dedicated hosts

QUESTION 5

Over 500 TB of data must be analyzed using standard SQL business intelligence tools. The dataset consists of a combination of structured data and unstructured data. The unstructured data is small and stored on Amazon S3. Which AWS services are most suitable for performing analytics on the data?

1. Amazon RDS MariaDB with Amazon Athena
2. Amazon DynamoDB with Amazon DynamoDB Accelerator (DAX)
3. Amazon ElastiCache for Redis with cluster mode enabled

4. Amazon Redshift with Amazon Redshift Spectrum

QUESTION 6

An application is being monitored using Amazon GuardDuty. A Solutions Architect needs to be notified by email of medium to high severity events. How can this be achieved?

1. Configure an Amazon CloudWatch alarm that triggers based on a GuardDuty metric
2. Create an Amazon CloudWatch events rule that triggers an Amazon SNS topic
3. Create an Amazon CloudWatch Logs rule that triggers an AWS Lambda function
4. Configure an Amazon CloudTrail alarm that triggers based on GuardDuty API activity

QUESTION 7

A company is migrating a decoupled application to AWS. The application uses a message broker based on the MQTT protocol. The application will be migrated to Amazon EC2 instances and the solution for the message broker must not require rewriting application code.

Which AWS service can be used for the migrated message broker?

1. Amazon SQS
2. Amazon SNS
3. Amazon MQ
4. AWS Step Functions

QUESTION 8

A HR application stores employment records on Amazon S3. Regulations mandate the records are retained for seven years. Once created the records are accessed infrequently for the first three months and then must be available within 10 minutes if required thereafter.

Which lifecycle action meets the requirements whilst MINIMIZING cost?

1. Store the data in S3 Standard for 3 months, then transition to S3 Glacier
2. Store the data in S3 Standard-IA for 3 months, then transition to S3 Glacier
3. Store the data in S3 Standard for 3 months, then transition to S3 Standard-IA
4. Store the data in S3 Intelligent Tiering for 3 months, then transition to S3 Standard-IA

QUESTION 9

A highly elastic application consists of three tiers. The application tier runs in an Auto Scaling group and processes data and writes it to an Amazon RDS MySQL database. The Solutions Architect wants to restrict access to the database tier to only accept traffic from the instances in the application tier. However, instances in the application tier are being constantly launched and terminated.

How can the Solutions Architect configure secure access to the database tier?

1. Configure the database security group to allow traffic only from the application security group
2. Configure the database security group to allow traffic only from port 3306
3. Configure a Network ACL on the database subnet to deny all traffic to ports other than 3306
4. Configure a Network ACL on the database subnet to allow all traffic from the application subnet

QUESTION 10

A Solutions Architect is rearchitecting an application with decoupling. The application will send batches of up to 1000 messages per second that must be received in the correct order by the consumers.

Which action should the Solutions Architect take?

1. Create an Amazon SQS Standard queue
2. Create an Amazon SNS topic
3. Create an Amazon SQS FIFO queue
4. Create an AWS Step Functions state machine

QUESTION 11

A Solutions Architect is designing an application that consists of AWS Lambda and Amazon RDS Aurora MySQL. The Lambda function must use database credentials to authenticate to MySQL and security policy mandates that these credentials must not be stored in the function code.

How can the Solutions Architect securely store the database credentials and make them available to the function?

1. Store the credentials in AWS Key Management Service and use environment variables in the function code pointing to KMS
2. Store the credentials in Systems Manager Parameter Store and update the function code and execution role
3. Use the AWSAuthenticationPlugin and associate an IAM user account in the MySQL database
4. Create an IAM policy and store the credentials in the policy. Attach the policy to the Lambda function execution role

QUESTION 12

A company are finalizing their disaster recovery plan. A limited set of core services will be replicated to the DR site ready to seamlessly take over in the event of a disaster. All other services will be switched off.

Which DR strategy is the company using?

1. Backup and restore
2. Pilot light
3. Warm standby
4. Multi-site

QUESTION 13

An application that runs a computational fluid dynamics workload uses a tightly-coupled HPC architecture that uses the MPI protocol and runs across many nodes. A service-managed deployment is required to minimize operational overhead.

Which deployment option is MOST suitable for provisioning and managing the resources required for this use case?

1. Use Amazon EC2 Auto Scaling to deploy instances in multiple subnets
2. Use AWS CloudFormation to deploy a Cluster Placement Group on EC2
3. Use AWS Batch to deploy a multi-node parallel job
4. Use AWS Elastic Beanstalk to provision and manage the EC2 instances

QUESTION 14

A Solutions Architect is designing an application that will run on an Amazon EC2 instance. The application must asynchronously invoke an AWS Lambda function to analyze thousands of .CSV files. The services should be decoupled.

Which service can be used to decouple the compute services?

1. Amazon SWF
2. Amazon SNS
3. Amazon Kinesis
4. Amazon OpsWorks

QUESTION 15

A large MongoDB database running on-premises must be migrated to Amazon DynamoDB within the next few weeks. The database is too large to migrate over the company's limited internet bandwidth so an alternative solution must be used. What should a Solutions Architect recommend?

1. Setup an AWS Direct Connect and migrate the database to Amazon DynamoDB using the AWS Database Migration Service (DMS)
2. Use the Schema Conversion Tool (SCT) to extract and load the data to an AWS Snowball Edge device. Use the AWS Database Migration Service (DMS) to migrate the data to Amazon DynamoDB
3. Enable compression on the MongoDB database and use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon DynamoDB
4. Use the AWS Database Migration Service (DMS) to extract and load the data to an AWS Snowball Edge device. Complete the migration to Amazon DynamoDB using AWS DMS in the AWS Cloud

QUESTION 16

Every time an item in an Amazon DynamoDB table is modified a record must be retained for compliance reasons. What is the most efficient solution to recording this information?

1. Enable Amazon CloudWatch Logs. Configure an AWS Lambda function to monitor the log files and record deleted item data to an Amazon S3 bucket
2. Enable DynamoDB Streams. Configure an AWS Lambda function to poll the stream and record the modified item data to an Amazon S3 bucket
3. Enable Amazon CloudTrail. Configure an Amazon EC2 instance to monitor activity in the CloudTrail log files and record changed items in another DynamoDB table
4. Enable DynamoDB Global Tables. Enable DynamoDB streams on the multi-region table and save the output directly to an Amazon S3 bucket

QUESTION 17

An application in a private subnet needs to query data in an Amazon DynamoDB table. Use of the DynamoDB public endpoints must be avoided. What is the most EFFICIENT and secure method of enabling access to the table?

1. Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)
2. Create a gateway VPC endpoint and add an entry to the route table
3. Create a private Amazon DynamoDB endpoint and connect to it using an AWS VPN
4. Create a software VPN between DynamoDB and the application in the private subnet

QUESTION 18

A Solutions Architect needs to select a low-cost, short-term option for adding resilience to an AWS Direct Connect connection. What is the MOST cost-effective solution to provide a backup for the Direct Connect connection?

1. Implement a second AWS Direct Connection
2. Implement an IPSec VPN connection and use the same BGP prefix
3. Configure AWS Transit Gateway with an IPSec VPN backup
4. Configure an IPSec VPN connection over the Direct Connect link

QUESTION 19

The disk configuration for an Amazon EC2 instance must be finalized. The instance will be running an application that requires heavy read/write IOPS. A single volume is required that is 500 GiB in size and needs to support 20,000 IOPS.

What EBS volume type should be selected?

1. EBS General Purpose SSD
2. EBS Provisioned IOPS SSD
3. EBS General Purpose SSD in a RAID 1 configuration
4. EBS Throughput Optimized HDD

QUESTION 20

A new application you are designing will store data in an Amazon Aurora MySQL DB. You are looking for a way to enable inter-region disaster recovery capabilities with fast replication and fast failover. Which of the following options is the BEST solution?

1. Use Amazon Aurora Global Database
2. Enable Multi-AZ for the Aurora DB
3. Create an EBS backup of the Aurora volumes and use cross-region replication to copy the snapshot
4. Create a cross-region Aurora Read Replica

QUESTION 21

A Solutions Architect regularly launches EC2 instances manually from the console and wants to streamline the process to reduce administrative overhead. Which feature of EC2 enables storing of settings such as AMI ID, instance type, key pairs and Security Groups?

1. Placement Groups

2. Launch Templates
3. Run Command
4. Launch Configurations

QUESTION 22

You recently noticed that your Network Load Balancer (NLB) in one of your VPCs is not distributing traffic evenly between EC2 instances in your AZs. There are an odd number of EC2 instances spread across two AZs. The NLB is configured with a TCP listener on port 80 and is using active health checks.

What is the most likely problem?

1. There is no HTTP listener
2. Health checks are failing in one AZ due to latency
3. NLB can only load balance within a single AZ
4. Cross-zone load balancing is disabled

QUESTION 23

A Solutions Architect is creating a design for a multi-tiered serverless application. Which two services form the application facing services from the AWS serverless infrastructure? (Select TWO.)

1. API Gateway
2. AWS Cognito
3. AWS Lambda
4. Amazon ECS
5. Elastic Load Balancer

QUESTION 24

A Solutions Architect attempted to restart a stopped EC2 instance and it immediately changed from a pending state to a terminated state. What are the most likely explanations? (Select TWO.)

1. You've reached your EBS volume limit
2. An EBS snapshot is corrupt
3. AWS does not currently have enough available On-Demand capacity to service your request
4. You have reached the limit on the number of instances that you can launch in a region
5. The AMI is unsupported

QUESTION 25

One of the applications you manage on RDS uses the MySQL DB and has been suffering from performance issues. You would like to setup a reporting process that will perform queries on the database but you're concerned that the extra load will further impact the performance of the DB and may lead to poor customer experience.

What would be the best course of action to take so you can implement the reporting process?

1. Configure Multi-AZ to setup a secondary database instance in another region
2. Deploy a Read Replica to setup a secondary read-only database instance
3. Deploy a Read Replica to setup a secondary read and write database instance
4. Configure Multi-AZ to setup a secondary database instance in another Availability Zone

QUESTION 26

A Solutions Architect is building a new Amazon Elastic Container Service (ECS) cluster. The ECS instances are running the EC2 launch type and load balancing is required to distribute connections to the tasks. It is required that the mapping of ports is performed dynamically and connections are routed to different groups of servers based on the path in the URL.

Which AWS service should the Solutions Architect choose to fulfil these requirements?

1. An Amazon ECS Service
2. Application Load Balancer
3. Network Load Balancer
4. Classic Load Balancer

QUESTION 27

A Solutions Architect needs to connect from an office location to a Linux instance that is running in a public subnet in an Amazon VPC using the Internet. Which of the following items are required to enable this access? (Select TWO.)

1. A bastion host
2. A NAT Gateway
3. A Public or Elastic IP address on the EC2 instance
4. An Internet Gateway attached to the VPC and route table attached to the public subnet pointing to it
5. An IPSec VPN

QUESTION 28

An Auto Scaling Group is unable to respond quickly enough to load changes resulting in lost messages from another application tier. The messages are typically around 128KB in size.

What is the best design option to prevent the messages from being lost?

1. Store the messages on Amazon S3
2. Launch an Elastic Load Balancer
3. Store the messages on an SQS queue
4. Use larger EC2 instance sizes

QUESTION 29

A Solutions Architect needs to run a production batch process quickly that will use several EC2 instances. The process cannot be interrupted and must be completed within a short time period.

What is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Reserved instances
2. Spot instances
3. Flexible instances
4. On-demand instances

QUESTION 30

A Solutions Architect would like to implement a method of automating the creation, retention, and deletion of backups for the Amazon EBS volumes in an Amazon VPC. What is the easiest way to automate these tasks using AWS tools?

1. Configure EBS volume replication to create a backup on Amazon S3
2. Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes
3. Create a scheduled job and run the AWS CLI command “create-backup” to take backups of the EBS volumes
4. Create a scheduled job and run the AWS CLI command “create-snapshot” to take backups of the EBS volumes

QUESTION 31

A mobile app uploads usage information to a database. Amazon Cognito is being used for authentication, authorization and user management and users sign-in with Facebook IDs.

In order to securely store data in DynamoDB, the design should use temporary AWS credentials. What feature of Amazon Cognito is used to obtain temporary credentials to access AWS services?

1. User Pools
2. Identity Pools
3. Key Pairs
4. SAML Identity Providers

QUESTION 32

A website uses web servers behind an Internet-facing Elastic Load Balancer. What record set should be created to point the customer’s DNS zone apex record at the ELB?

1. Create a PTR record pointing to the DNS name of the load balancer
2. Create an A record pointing to the DNS name of the load balancer

3. Create a CNAME record that is an Alias, and select the ELB DNS as a target
4. Create an A record that is an Alias, and select the ELB DNS as a target

QUESTION 33

A Solutions Architect has been assigned the task of moving some sensitive documents into the AWS cloud. The security of the documents must be maintained.

Which AWS features can help ensure that the sensitive documents cannot be read even if they are compromised? (Select TWO.)

1. AWS IAM Access Policy
2. Amazon S3 Server-Side Encryption
3. Amazon EBS snapshots
4. Amazon S3 cross region replication
5. Amazon EBS encryption with Customer Managed Keys

QUESTION 34

A membership website has become quite popular and is gaining members quickly. The website currently runs on Amazon EC2 instances with one web server instance and one database instance running MySQL. A Solutions Architect is concerned about the lack of high-availability in the current architecture.

What can the Solutions Architect do to easily enable high availability without making major changes to the architecture?

1. Create a Read Replica in another availability zone
2. Enable Multi-AZ for the MySQL instance
3. Install MySQL on an EC2 instance in the same availability zone and enable replication
4. Install MySQL on an EC2 instance in another availability zone and enable replication

QUESTION 35

A Solutions Architect has setup a VPC with a public subnet and a VPN-only subnet. The public subnet is associated with a custom route table that has a route to an Internet Gateway. The VPN-only subnet is associated with the main route table and has a route to a virtual private gateway.

The Architect has created a new subnet in the VPC and launched an EC2 instance in it. However, the instance cannot connect to the Internet. What is the MOST likely reason?

1. The subnet has been automatically associated with the main route table which does not have a route to the Internet
2. The new subnet has not been associated with a route table
3. The Internet Gateway is experiencing connectivity problems
4. There is no NAT Gateway available in the new subnet so Internet connectivity is not possible

QUESTION 36

A customer has a public-facing web application hosted on a single Amazon Elastic Compute Cloud (EC2) instance serving videos directly from an Amazon S3 bucket. Which of the following will restrict third parties from directly accessing the video assets in the bucket?

1. Launch the website Amazon EC2 instance using an IAM role that is authorized to access the videos
2. Restrict access to the bucket to the public CIDR range of the company locations
3. Use a bucket policy to only allow referrals from the main website URL
4. Use a bucket policy to only allow the public IP address of the Amazon EC2 instance hosting the customer website

QUESTION 37

A Solutions Architect is creating an AWS CloudFormation template that will provision a new EC2 instance and new EBS volume. What must be specified to associate the block store with the instance?

1. Both the EC2 physical ID and the EBS physical ID
2. The EC2 physical ID
3. Both the EC2 logical ID and the EBS logical ID
4. The EC2 logical ID

QUESTION 38

An application stores encrypted data in Amazon S3 buckets. A Solutions Architect needs to be able to query the encrypted data using SQL queries and write the encrypted results back to the S3 bucket. As the data is sensitive fine-grained control must be implemented over access to the S3 bucket.

What combination of services represent the BEST options support these requirements? (Select TWO.)

1. Use AWS Glue to extract the data, analyze it, and load it back to the S3 bucket
2. Use bucket ACLs to restrict access to the bucket
3. Use IAM policies to restrict access to the bucket
4. Use Athena for querying the data and writing the results back to the bucket
5. Use the AWS KMS API to query the encrypted data, and the S3 API for writing the results

QUESTION 39

A Solutions Architect works for a systems integrator running a platform that stores medical records. The government security policy mandates that patient data that contains personally identifiable information (PII) must be encrypted at all times, both at rest and in transit. Amazon S3 is used to back up data into the AWS cloud.

How can the Solutions Architect ensure the medical records are properly secured? (Select TWO.)

1. Before uploading the data to S3 over HTTPS, encrypt the data locally using your own encryption keys
2. Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-128
3. Attach an encrypted EBS volume to an EC2 instance
4. Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-256
5. Upload the data using CloudFront with an EC2 origin

QUESTION 40

A Solutions Architect is considering the best approach to enabling Internet access for EC2 instances in a private subnet. What advantages do NAT Gateways have over NAT Instances? (Select TWO.)

1. Can be assigned to security groups
2. Can be used as a bastion host
3. Managed for you by AWS
4. Highly available within each AZ
5. Can be scaled up manually

QUESTION 41

A Solutions Architect must design a solution for providing single sign-on to existing staff in a company. The staff manage on-premise web applications and also need access to the AWS management console to manage resources in the AWS cloud.

Which combination of services are BEST suited to delivering these requirements?

1. Use IAM and Amazon Cognito
2. Use your on-premise LDAP directory with IAM
3. Use the AWS Secure Token Service (STS) and SAML
4. Use IAM and MFA

QUESTION 42

A Solutions Architect is designing a three-tier web application that includes an Auto Scaling group of Amazon EC2 Instances running behind an Elastic Load Balancer. The security team requires that all web servers must be accessible only through the Elastic Load Balancer and that none of the web servers are directly accessible from the Internet.

How should the Architect meet these requirements?

1. Create an Amazon CloudFront distribution in front of the Elastic Load Balancer
2. Configure the web servers' security group to deny traffic from the Internet
3. Configure the web tier security group to allow only traffic from the Elastic Load Balancer
4. Install a Load Balancer on an Amazon EC2 instance

QUESTION 43

A Solutions Architect is creating a URL that lets users who sign in to the organization's network securely access the AWS Management Console. The URL will include a sign-in token that authenticates the user to AWS. Microsoft Active Directory Federation Services is being used as the identity provider (IdP).

Which of the steps below will the Solutions Architect need to include when developing the custom identity broker? (Select TWO.)

1. Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token
2. Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
3. Assume an IAM Role through the console or programmatically with the AWS CLI, Tools for Windows PowerShell or API
4. Generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET
5. Delegate access to the IdP through the "Configure Provider" wizard in the IAM console

QUESTION 44

Some Amazon ECS containers are running on a cluster using the EC2 launch type. The current configuration uses the container instance's IAM roles for assigning permissions to the containerized applications.

A Solutions Architect needs to implement more granular permissions so that some applications can be assigned more restrictive permissions. How can this be achieved?

1. This cannot be changed as IAM roles can only be linked to container instances
2. This can be achieved using IAM roles for tasks, and splitting the containers according to the permissions required to different task definition profiles
3. This can be achieved by configuring a resource-based policy for each application
4. This can only be achieved using the Fargate launch type

QUESTION 45

An application uses a combination of Reserved and On-Demand instances to handle typical load. The application involves performing analytics on a set of data. A Solutions Architect needs to temporarily deploy a large number of EC2 instances. The instances must be available for a short period of time until the analytics job is completed.

If job completion is not time-critical, what is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Use Spot instances
2. Use dedicated hosts
3. Use On-Demand instances
4. Use Reserved instances

QUESTION 46

There is a problem with an EC2 instance that was launched by Amazon EC2 Auto Scaling. The EC2 status checks have reported that the instance is "Impaired". What action will EC2 Auto Scaling take?

1. Auto Scaling will perform Availability Zone rebalancing
2. It will wait a few minutes for the instance to recover and if it does not it will mark the instance for termination, terminate it, and then launch a replacement
3. Auto Scaling performs its own status checks and does not integrate with EC2 status checks
4. It will launch a new instance immediately and then mark the impaired one for replacement

QUESTION 47

A pharmaceutical company uses a strict process for release automation that involves building and testing services in 3 separate VPCs. A peering topology is configured with VPC-A peered with VPC-B and VPC-B peered with VPC-C. The development team wants to modify the process so that they can release code directly from VPC-A to VPC-C.

How can this be accomplished?

1. Update VPC-Bs route table with peering targets for VPC-A and VPC-C and enable route propagation

2. Create a new VPC peering connection between VPC-A and VPC-C
3. Update the CIDR blocks to match to enable inter-VPC routing
4. Update VPC-As route table with an entry using the VPC peering as a target

QUESTION 48

A Solutions Architect needs to work programmatically with IAM. Which feature of IAM allows direct access to the IAM web service using HTTPS to call service actions and what is the method of authentication that must be used? (Select TWO.)

1. OpenID Connect
2. Query API
3. API Gateway
4. Access key ID and secret access key
5. IAM role

QUESTION 49

The Systems Administrators in a company currently use Chef for configuration management of on-premise servers. Which AWS service can a Solutions Architect use that will provide a fully-managed configuration management service that will enable the use of existing Chef cookbooks?

1. Elastic Beanstalk
2. CloudFormation
3. OpsWorks for Chef Automate
4. Opsworks Stacks

QUESTION 50

An Amazon RDS Multi-AZ deployment is running in an Amazon VPC. An outage occurs in the availability zone of the primary RDS database instance. What actions will take place in this circumstance? (Select TWO.)

1. The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance
2. A failover will take place once the connection draining timer has expired
3. A manual failover of the DB instance will need to be initiated using Reboot with failover
4. The primary DB instance will switch over automatically to the standby replica
5. Due to the loss of network connectivity the process to switch to the standby replica cannot take place

QUESTION 51

A Solutions Architect is designing a web-facing application. The application will run on Amazon EC2 instances behind Elastic Load Balancers in multiple regions in an active/passive configuration. The website address the application runs on is example.com. AWS Route 53 will be used to perform DNS resolution for the application.

How should the Solutions Architect configure AWS Route 53 in this scenario based on AWS best practices? (Select TWO.)

1. Use a Failover Routing Policy
2. Set Evaluate Target Health to “No” for the primary
3. Use a Weighted Routing Policy
4. Connect the ELBs using Alias records
5. Connect the ELBs using CNAME records

QUESTION 52

A Solutions Architect is designing a new retail website for a high-profile company. The company has previously been the victim of targeted distributed denial-of-service (DDoS) attacks and has requested that the design includes mitigation techniques.

Which of the following are the BEST techniques to help ensure the availability of the services is not compromised in an attack? (Select TWO.)

1. Configure Auto Scaling with a high maximum number of instances to ensure it can scale accordingly
2. Use CloudFront for distributing both static and dynamic content
3. Use Spot instances to reduce the cost impact in case of attack
4. Use encryption on your EBS volumes

5. Use Placement Groups to ensure high bandwidth and low latency

QUESTION 53

An application running on Amazon EC2 requires an EBS volume for saving structured data. The application vendor suggests that the performance of the disk should be up to 3 IOPS per GB. The capacity is expected to grow to 2 TB.

Taking into account cost effectiveness, which EBS volume type should be used?

1. Throughput Optimized HDD (ST1)
2. General Purpose (GP2)
3. Provisioned IOPS (Io1)
4. Cold HDD (SC1)

QUESTION 54

An application in an Amazon VPC uses an Auto Scaling Group that spans 3 AZs and there are currently 4 Amazon EC2 instances running in the group. What actions will Auto Scaling take, by default, if it needs to terminate an EC2 instance?

1. Randomly select one of the 3 AZs, and then terminate an instance in that AZ
2. Terminate the instance with the least active network connections. If multiple instances meet this criterion, one will be randomly selected
3. Send an SNS notification, if configured to do so
4. Wait for the cooldown period and then terminate the instance that has been running the longest
5. Terminate an instance in the AZ which currently has 2 running EC2 instances

QUESTION 55

Several environments are being created in a single Amazon VPC. The Solutions Architect needs to implement a system of categorization that allows for identification of Amazon EC2 resources by business unit, owner, or environment.

Which AWS feature can be used?

1. Parameters
2. Metadata
3. Custom filters
4. Tags

QUESTION 56

An organization has a data lake on Amazon S3 and needs to find a solution for performing in-place queries of the data assets in the data lake. The requirement is to perform both data discovery and SQL querying, and complex queries from a large number of concurrent users using BI tools.

What is the BEST combination of AWS services to use in this situation? (Select TWO.)

1. RedShift Spectrum for the complex queries
2. Amazon Athena for the ad hoc SQL querying
3. AWS Glue for the ad hoc SQL querying
4. AWS Lambda for the complex queries
5. Amazon Kinesis for the complex queries

QUESTION 57

When using throttling controls with API Gateway what happens when request submissions exceed the steady-state request rate and burst limits?

1. API Gateway fails the limit-exceeding requests and returns “429 Too Many Requests” error responses to the client
2. The requests will be buffered in a cache until the load reduces
3. API Gateway drops the requests and does not return a response to the client
4. API Gateway fails the limit-exceeding requests and returns “500 Internal Server Error” error responses to the client

QUESTION 58

A Solutions Architect created a new VPC and setup an Auto Scaling Group to maintain a desired count of 2 Amazon EC2 instances. The security team has requested that the EC2 instances be located in a private subnet. To distribute load, an Internet-facing Application Load Balancer (ALB) is also required.

With the security team's requirements in mind, what else needs to be done to get this configuration to work? (Select TWO.)

1. Attach an Internet Gateway to the private subnets
2. Associate the public subnets with the ALB
3. Add an Elastic IP address to each EC2 instance in the private subnet
4. Add a NAT gateway to the private subnet
5. For each private subnet create a corresponding public subnet in the same AZ

QUESTION 59

An application running AWS uses an Elastic Load Balancer (ELB) to distribute connections between EC2 instances. A Solutions Architect needs to record information on the requester, IP, and request type for connections made to the ELB. Additionally, the Architect will also need to perform some analysis on the log files.

Which AWS services and configuration options can be used to collect and then analyze the logs? (Select TWO.)

1. Use EMR for analyzing the log files
2. Update the application to use DynamoDB for storing log files
3. Use Elastic Transcoder to analyze the log files
4. Enable Access Logs on the ELB and store the log files on S3
5. Enable Access Logs on the EC2 instances and store the log files on S3

QUESTION 60

A Solutions Architect would like to store a backup of an Amazon EBS volume on Amazon S3. What is the easiest way of achieving this?

1. Use SWF to automatically create a backup of your EBS volumes and then upload them to an S3 bucket
2. You don't need to do anything, EBS volumes are automatically backed up by default
3. Write a custom script to automatically copy your data to an S3 bucket
4. Create a snapshot of the volume

QUESTION 61

An application will gather data from a website hosted on an EC2 instance and write the data to an S3 bucket. The application will use API calls to interact with the EC2 instance and S3 bucket.

Which Amazon S3 access control method will be the MOST operationally efficient? (Select TWO.)

1. Create a bucket policy
2. Grant programmatic access
3. Use key pairs
4. Grant AWS Management Console access
5. Create an IAM policy

QUESTION 62

An Amazon CloudWatch alarm recently notified a Solutions Architect that the load on an Amazon DynamoDB table is getting close to the provisioned capacity for writes. The DynamoDB table is part of a two-tier customer-facing application and is configured using provisioned capacity.

What will happen if the limit for the provisioned capacity for writes is reached?

1. The requests will be throttled, and fail with an HTTP 503 code (Service Unavailable)
2. DynamoDB scales automatically so there's no need to worry
3. The requests will be throttled, and fail with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceededException
4. The requests will succeed, and an HTTP 200 status code will be returned

QUESTION 63

A Solutions Architect is creating the business process workflows associated with an order fulfilment system. What AWS service can assist with coordinating tasks across distributed application components?

1. AWS STS
2. Amazon SQS
3. Amazon SWF
4. Amazon SNS

QUESTION 64

An EC2 instance in an Auto Scaling group is having some issues that are causing it to launch new instances based on the dynamic scaling policy. A Solutions Architect needs to troubleshoot the EC2 instance and prevent the Auto Scaling group from launching new instances temporarily.

What is the best method to accomplish this? (Select TWO.)

1. Remove the EC2 instance from the Target Group
2. Disable the launch configuration associated with the EC2 instance
3. Place the EC2 instance that is experiencing issues into the Standby state
4. Suspend the scaling processes responsible for launching new instances
5. Disable the dynamic scaling policy

QUESTION 65

An Amazon VPC has been deployed with private and public subnets. A MySQL database server running on an Amazon EC2 instance will soon be launched. According to AWS best practice, which subnet should the database server be launched into?

1. It doesn't matter
2. The private subnet
3. The public subnet
4. The subnet that is mapped to the primary AZ in the region

SET 4: PRACTICE QUESTIONS AND ANSWERS

QUESTION 1

A company is deploying an Amazon ElastiCache for Redis cluster. To enhance security a password should be required to access the database. What should the solutions architect use?

1. AWS Directory Service
2. AWS IAM Policy
3. Redis AUTH command
4. VPC Security Group

Answer: 3

Explanation:

Redis authentication tokens enable Redis to require a token (password) before allowing clients to execute commands, thereby improving data security.

You can require that users enter a token on a token-protected Redis server. To do this, include the parameter --auth-token (API: AuthToken) with the correct token when you create your replication group or cluster. Also include it in all subsequent commands to the replication group or cluster.

CORRECT: "Redis AUTH command" is the correct answer.

INCORRECT: "AWS Directory Service" is incorrect. This is a managed Microsoft Active Directory service and cannot add password protection to Redis.

INCORRECT: "AWS IAM Policy" is incorrect. You cannot use an IAM policy to enforce a password on Redis.

INCORRECT: "VPC Security Group" is incorrect. A security group protects at the network layer, it does not affect application authentication.

References:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticsearch/>

QUESTION 2

To increase performance and redundancy for an application a company has decided to run multiple implementations in different AWS Regions behind network load balancers. The company currently advertise the application using two public IP addresses from separate /24 address ranges and would prefer not to change these. Users should be directed to the closest available application endpoint.

Which actions should a solutions architect take? (Select TWO.)

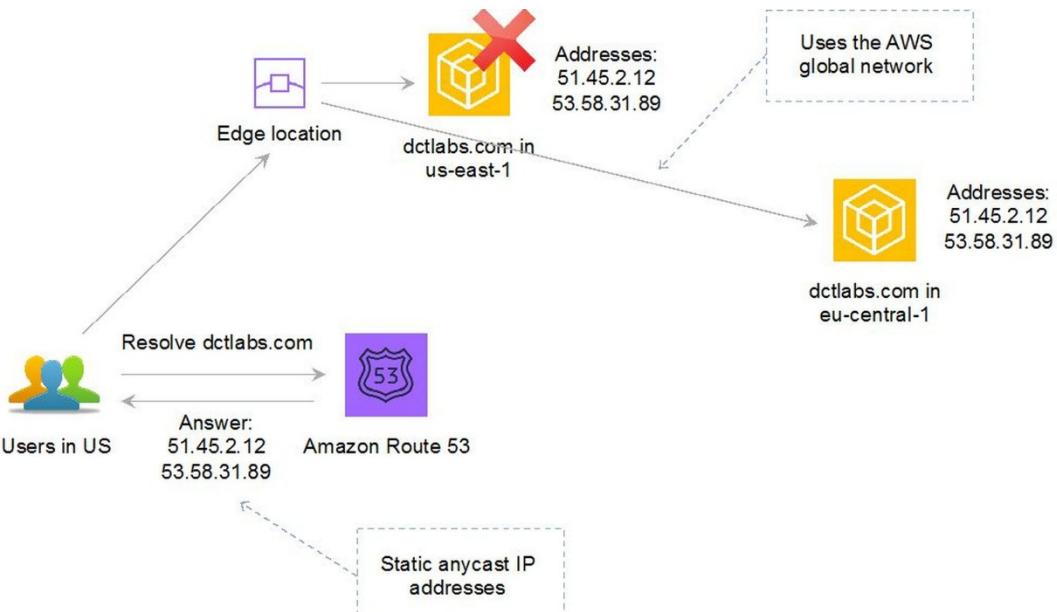
1. Create an Amazon Route 53 geolocation based routing policy
2. Create an AWS Global Accelerator and attach endpoints in each AWS Region
3. Assign new static anycast IP addresses and modify any existing pointers
4. Migrate both public IP addresses to the AWS Global Accelerator
5. Create PTR records to map existing public IP addresses to an Alias

Answer: 2,4

Explanation:

AWS Global Accelerator uses static IP addresses as fixed entry points for your application. You can migrate up to two /24 IPv4 address ranges and choose which /32 IP addresses to use when you create your accelerator.

This solution ensures the company can continue using the same IP addresses and they are able to direct traffic to the application endpoint in the AWS Region closest to the end user. Traffic is sent over the AWS global network for consistent performance.



CORRECT: "Create an AWS Global Accelerator and attach endpoints in each AWS Region" is a correct answer.

CORRECT: "Migrate both public IP addresses to the AWS Global Accelerator" is also a correct answer.

INCORRECT: "Create an Amazon Route 53 geolocation based routing policy" is incorrect. With this solution new IP addresses will be required as there will be application endpoints in different regions.

INCORRECT: "Assign new static ancast IP addresses and modify any existing pointers" is incorrect. This is unnecessary as you can bring your own IP addresses to AWS Global Accelerator and this is preferred in this scenario.

INCORRECT: "Create PTR records to map existing public IP addresses to an Alias" is incorrect. This is not a workable solution for mapping existing IP addresses to an Amazon Route 53 Alias.

References:

<https://aws.amazon.com/global-accelerator/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-global-accelerator/>

QUESTION 3

Three Amazon VPCs are used by a company in the same region. The company has two AWS Direct Connect connections to two separate company offices and wishes to share these with all three VPCs. A Solutions Architect has created an AWS Direct Connect gateway. How can the required connectivity be configured?

1. Associate the Direct Connect gateway to a transit gateway
2. Associate the Direct Connect gateway to a virtual private gateway in each VPC
3. Create a VPC peering connection between the VPCs and route entries for the Direct Connect Gateway
4. Create a transit virtual interface between the Direct Connect gateway and each VPC

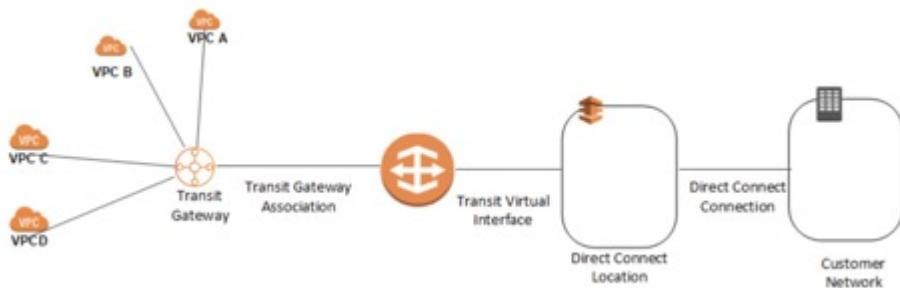
Answer: 1

Explanation:

You can manage a single connection for multiple VPCs or VPNs that are in the same Region by associating a Direct Connect gateway to a transit gateway. The solution involves the following components:

- A transit gateway that has VPC attachments.
- A Direct Connect gateway.
- An association between the Direct Connect gateway and the transit gateway.
- A transit virtual interface that is attached to the Direct Connect gateway.

The following diagram depicts this configuration:



CORRECT: "Associate the Direct Connect gateway to a transit gateway" is the correct answer.

INCORRECT: "Associate the Direct Connect gateway to a virtual private gateway in each VPC" is incorrect. For VPCs in the same region a VPG is not necessary. A transit gateway can instead be configured.

INCORRECT: "Create a VPC peering connection between the VPCs and route entries for the Direct Connect Gateway" is incorrect. You cannot add route entries for a Direct Connect gateway to each VPC and enable routing. Use a transit gateway instead.

INCORRECT: "Create a transit virtual interface between the Direct Connect gateway and each VPC" is incorrect. The transit virtual interface is attached to the Direct Connect gateway on the connection side, not the VPC/transit gateway side.

References:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

QUESTION 4

A retail organization sends coupons out twice a week and this results in a predictable surge in sales traffic. The application runs on Amazon EC2 instances behind an Elastic Load Balancer. The organization is looking for ways lower costs while ensuring they meet the demands of their customers.

How can they achieve this goal?

1. Use capacity reservations with savings plans
2. Use a mixture of spot instances and on demand instances
3. Increase the instance size of the existing EC2 instances
4. Purchase Amazon EC2 dedicated hosts

Answer: 1

Explanation:

On-Demand Capacity Reservations enable you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration. By creating Capacity Reservations, you ensure that you always have access to EC2 capacity when you need it, for as long as you need it. When used in combination with savings plans, you can also gain the advantages of cost reduction.

CORRECT: " Use capacity reservations with savings plans" is the correct answer.

INCORRECT: "Use a mixture of spot instances and on demand instances" is incorrect. You can mix spot and on-demand in an auto scaling group. However, there's a risk the spot price may not be good, and this is a regular, predictable increase in traffic.

INCORRECT: "Increase the instance size of the existing EC2 instances" is incorrect. This would add more cost all the time rather than catering for the temporary increases in traffic.

INCORRECT: "Purchase Amazon EC2 dedicated hosts" is incorrect. This is not a way to save cost as dedicated hosts are much more expensive than shared hosts.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html#capacity-reservations-differences>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 5

Over 500 TB of data must be analyzed using standard SQL business intelligence tools. The dataset consists of a combination of structured data and unstructured data. The unstructured data is small and stored on Amazon S3. Which AWS services are most suitable for performing analytics on the data?

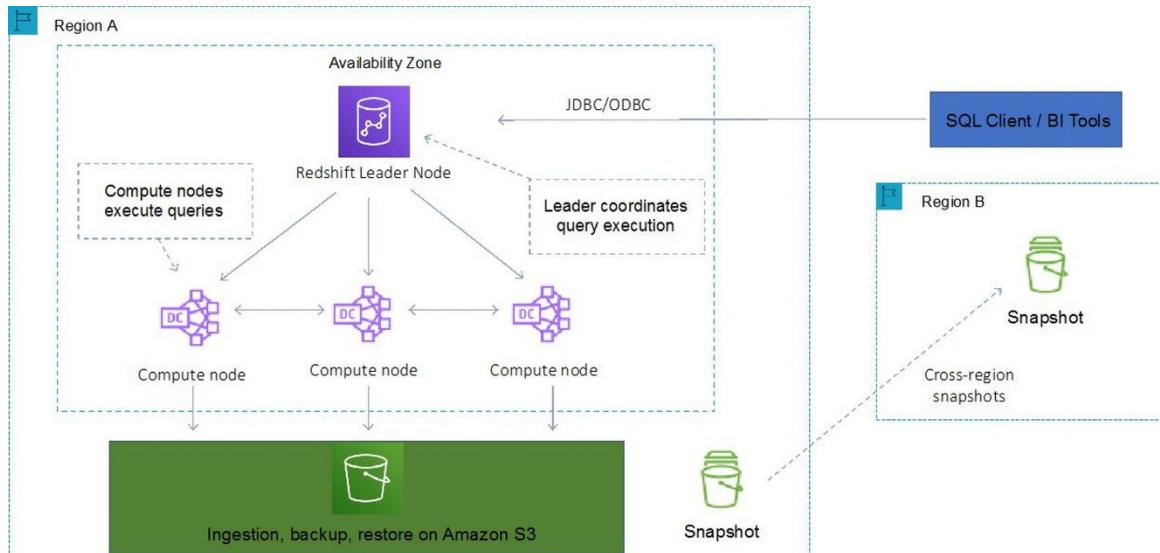
1. Amazon RDS MariaDB with Amazon Athena
2. Amazon DynamoDB with Amazon DynamoDB Accelerator (DAX)
3. Amazon ElastiCache for Redis with cluster mode enabled
4. Amazon Redshift with Amazon Redshift Spectrum

Answer: 4

Explanation:

Amazon Redshift is an enterprise-level, petabyte scale, fully managed data warehousing service. An Amazon Redshift data warehouse is an enterprise-class relational database query and management system. Redshift supports client connections with many types of applications, including business intelligence (BI), reporting, data, and analytics tools.

Using Amazon Redshift Spectrum, you can efficiently query and retrieve structured and semistructured data from files in Amazon S3 without having to load the data into Amazon Redshift tables. Redshift Spectrum queries employ massive parallelism to execute very fast against large datasets.



Used together, RedShift and RedShift spectrum are suitable for running massive analytics jobs on both the structured (RedShift data warehouse) and unstructured (Amazon S3) data.

CORRECT: "Amazon Redshift with Amazon Redshift Spectrum" is the correct answer.

INCORRECT: "Amazon RDS MariaDB with Amazon Athena" is incorrect. Amazon RDS is not suitable for analytics (OLAP) use cases as it is designed for transactional (OLTP) use cases. Athena can however be used for running SQL queries on data on S3.

INCORRECT: "Amazon DynamoDB with Amazon DynamoDB Accelerator (DAX)" is incorrect. This is an example of a non-relational DB with a caching layer and is not suitable for an OLAP use case.

INCORRECT: "Amazon ElastiCache for Redis with cluster mode enabled" is incorrect. This is an example of an in-memory caching service. It is good for performance for transactional use cases.

References:

https://docs.aws.amazon.com/redshift/latest/dg/c_redshift_system_overview.html

<https://docs.aws.amazon.com/redshift/latest/dg/c-using-spectrum.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>

QUESTION 6

An application is being monitored using Amazon GuardDuty. A Solutions Architect needs to be notified by email of medium to high severity events. How can this be achieved?

1. Configure an Amazon CloudWatch alarm that triggers based on a GuardDuty metric
2. Create an Amazon CloudWatch events rule that triggers an Amazon SNS topic
3. Create an Amazon CloudWatch Logs rule that triggers an AWS Lambda function
4. Configure an Amazon CloudTrail alarm that triggers based on GuardDuty API activity

Answer: 2

Explanation:

A CloudWatch Events rule can be used to set up automatic email notifications for Medium to High Severity findings to the email address of your choice. You simply create an Amazon SNS topic and then associate it with an Amazon CloudWatch events rule.

Note: step by step procedures for how to set this up can be found in the article linked in the references below.

CORRECT: "Create an Amazon CloudWatch events rule that triggers an Amazon SNS topic" is the correct answer.

INCORRECT: "Configure an Amazon CloudWatch alarm that triggers based on a GuardDuty metric" is incorrect. There is no metric for GuardDuty that can be used for specific findings.

INCORRECT: "Create an Amazon CloudWatch Logs rule that triggers an AWS Lambda function" is incorrect. CloudWatch logs is not the right CloudWatch service to use. CloudWatch events is used for reacting to changes in service state.

INCORRECT: "Configure an Amazon CloudTrail alarm that triggers based on GuardDuty API activity" is incorrect. CloudTrail cannot be used to trigger alarms based on GuardDuty API activity.

References:

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/>

QUESTION 7

A company is migrating a decoupled application to AWS. The application uses a message broker based on the MQTT protocol. The application will be migrated to Amazon EC2 instances and the solution for the message broker must not require rewriting application code.

Which AWS service can be used for the migrated message broker?

1. Amazon SQS
2. Amazon SNS
3. Amazon MQ
4. AWS Step Functions

Answer: 3

Explanation:

Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Connecting current applications to Amazon MQ is easy because it uses industry-standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket. Using standards means that in most cases, there's no need to rewrite any messaging code when you migrate to AWS.

CORRECT: "Amazon MQ" is the correct answer.

INCORRECT: "Amazon SQS" is incorrect. This is an Amazon proprietary service and does not support industry-standard messaging APIs and protocols.

INCORRECT: "Amazon SNS" is incorrect. This is a notification service not a message bus.

INCORRECT: "AWS Step Functions" is incorrect. This is a workflow orchestration service, not a message bus.

References:

<https://aws.amazon.com/amazon-mq/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-mq/>

QUESTION 8

A HR application stores employment records on Amazon S3. Regulations mandate the records are retained for seven years. Once created the records are accessed infrequently for the first three months and then must be available within 10 minutes if required thereafter.

Which lifecycle action meets the requirements whilst MINIMIZING cost?

1. Store the data in S3 Standard for 3 months, then transition to S3 Glacier
2. Store the data in S3 Standard-IA for 3 months, then transition to S3 Glacier
3. Store the data in S3 Standard for 3 months, then transition to S3 Standard-IA
4. Store the data in S3 Intelligent Tiering for 3 months, then transition to S3 Standard-IA

Answer: 2

Explanation:

The most cost-effective solution is to first store the data in S3 Standard-IA where it will be infrequently accessed for the first three months. Then, after three months expires, transition the data to S3 Glacier where it can be stored at lower cost for the remainder of the seven year period. Expedited retrieval can bring retrieval times down to 1-5 minutes.

CORRECT: "Store the data in S3 Standard-IA for 3 months, then transition to S3 Glacier" is the correct answer.

INCORRECT: "Store the data in S3 Standard for 3 months, then transition to S3 Glacier" is incorrect. S3 Standard is more costly than S3 Standard-IA and the data is only accessed infrequently.

INCORRECT: "Store the data in S3 Standard for 3 months, then transition to S3 Standard-IA" is incorrect. Neither storage class in this answer is the most cost-effective option.

INCORRECT: "Store the data in S3 Intelligent Tiering for 3 months, then transition to S3 Standard-IA" is incorrect. Intelligent tiering moves data between tiers based on access patterns, this is more costly and better suited to use cases that are unknown or unpredictable.

References:

<https://aws.amazon.com/s3/storage-classes/>

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

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 9

A highly elastic application consists of three tiers. The application tier runs in an Auto Scaling group and processes data and writes it to an Amazon RDS MySQL database. The Solutions Architect wants to restrict access to the database tier to only accept traffic from the instances in the application tier. However, instances in the application tier are being constantly launched and terminated.

How can the Solutions Architect configure secure access to the database tier?

1. Configure the database security group to allow traffic only from the application security group
2. Configure the database security group to allow traffic only from port 3306
3. Configure a Network ACL on the database subnet to deny all traffic to ports other than 3306
4. Configure a Network ACL on the database subnet to allow all traffic from the application subnet

Answer: 1

Explanation:

The best option is to configure the database security group to only allow traffic that originates from the application security group. You can also define the destination port as the database port. This setup will allow any instance that is launched and attached to this security group to connect to the database.

CORRECT: "Configure the database security group to allow traffic only from the application security group" is the correct answer.

INCORRECT: "Configure the database security group to allow traffic only from port 3306" is incorrect. Port 3306 for MySQL should be the destination port, not the source.

INCORRECT: "Configure a Network ACL on the database subnet to deny all traffic to ports other than 3306" is incorrect. This does not restrict access specifically to the application instances.

INCORRECT: "Configure a Network ACL on the database subnet to allow all traffic from the application subnet" is incorrect. This does not restrict access specifically to the application instances.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 10

A Solutions Architect is rearchitecting an application with decoupling. The application will send batches of up to 1000 messages per second that must be received in the correct order by the consumers.

Which action should the Solutions Architect take?

1. Create an Amazon SQS Standard queue
2. Create an Amazon SNS topic
3. Create an Amazon SQS FIFO queue
4. Create an AWS Step Functions state machine

Answer: 3

Explanation:

Only FIFO queues guarantee the ordering of messages and therefore a standard queue would not work. The FIFO queue supports up to 3,000 messages per second with batching so this is a supported scenario.

Standard Queue	FIFO Queue
Unlimited Throughput: Standard queues support a nearly unlimited number of transactions per second (TPS) per API action.	High Throughput: FIFO queues support up to 300 messages per second (300 send, receive, or delete operations per second). When you batch 10 messages per operation (maximum), FIFO queues can support up to 3,000 messages per second
Best-Effort Ordering: Occasionally, messages might be delivered in an order different from which they were sent	First-In-First-out Delivery: The order in which messages are sent and received is strictly preserved
At-Least-Once Delivery: A message is delivered at least once, but occasionally more than one copy of a message is delivered	Exactly-Once Processing: A message is delivered once and remains available until a consumer processes and deletes it. Duplicates are not introduced into the queue

CORRECT: "Create an Amazon SQS FIFO queue" is the correct answer.

INCORRECT: "Create an Amazon SQS Standard queue" is incorrect as it does not guarantee ordering of messages.

INCORRECT: "Create an Amazon SNS topic" is incorrect. SNS is a notification service and a message queue is a better fit for this use case.

INCORRECT: "Create an AWS Step Functions state machine" is incorrect. Step Functions is a workflow orchestration service and is not useful for this scenario.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-quotas.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 11

A Solutions Architect is designing an application that consists of AWS Lambda and Amazon RDS Aurora MySQL. The Lambda function must use database credentials to authenticate to MySQL and security policy mandates that these credentials must not be stored in the function code.

How can the Solutions Architect securely store the database credentials and make them available to the function?

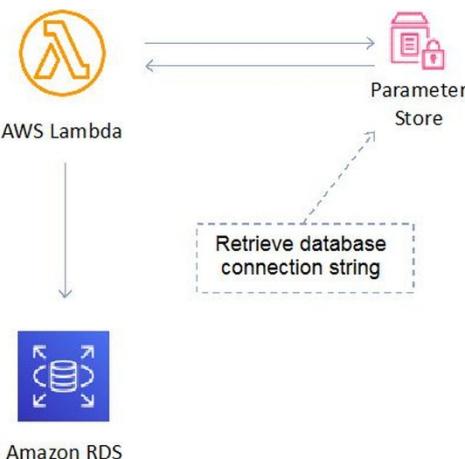
1. Store the credentials in AWS Key Management Service and use environment variables in the function code pointing to KMS
2. Store the credentials in Systems Manager Parameter Store and update the function code and execution role
3. Use the AWSAuthenticationPlugin and associate an IAM user account in the MySQL database
4. Create an IAM policy and store the credentials in the policy. Attach the policy to the Lambda function execution role

Answer: 2

Explanation:

In this case the scenario requires that credentials are used for authenticating to MySQL. The credentials need to be securely stored outside of the function code. Systems Manager Parameter Store provides secure, hierarchical storage for configuration data management and secrets management.

You can easily reference the parameters from services including AWS Lambda as depicted in the diagram below:



CORRECT: "Store the credentials in Systems Manager Parameter Store and update the function code and execution role" is the correct answer.

INCORRECT: "Store the credentials in AWS Key Management Service and use environment variables in the function code pointing to KMS" is incorrect. You cannot store credentials in KMS, it is used for creating and managing encryption keys

INCORRECT: "Use the AWSAuthenticationPlugin and associate an IAM user account in the MySQL database" is incorrect. This is a great way to securely authenticate to RDS using IAM users or roles. However, in this case the scenario requires database credentials to be used by the function.

INCORRECT: "Create an IAM policy and store the credentials in the policy. Attach the policy to the Lambda function execution role" is incorrect. You cannot store credentials in IAM policies.

References:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html>

QUESTION 12

A company are finalizing their disaster recovery plan. A limited set of core services will be replicated to the DR site ready to seamlessly take over the in the event of a disaster. All other services will be switched off.

Which DR strategy is the company using?

1. Backup and restore
2. Pilot light
3. Warm standby
4. Multi-site

Answer: 2

Explanation:

In this DR approach, you simply replicate part of your IT structure for a limited set of core services so that the AWS cloud environment seamlessly takes over in the event of a disaster.

A small part of your infrastructure is always running simultaneously syncing mutable data (as databases or documents), while other parts of your infrastructure are switched off and used only during testing.

Unlike a backup and recovery approach, you must ensure that your most critical core elements are already configured and running in AWS (the pilot light). When the time comes for recovery, you can rapidly provision a full-scale production environment around the critical core.

CORRECT: "Pilot light" is the correct answer.

INCORRECT: "Backup and restore" is incorrect. This is the lowest cost DR approach that simply entails creating online backups of all data and applications.

INCORRECT: "Warm standby" is incorrect. The term warm standby is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud.

INCORRECT: "Multi-site" is incorrect. A multi-site solution runs on AWS as well as on your existing on-site infrastructure in an active-active configuration.

References:

<https://aws.amazon.com/blogs/publicsector/rapidly-recover-mission-critical-systems-in-a-disaster/>

QUESTION 13

An application that runs a computational fluid dynamics workload uses a tightly-coupled HPC architecture that uses the MPI protocol and runs across many nodes. A service-managed deployment is required to minimize operational overhead.

Which deployment option is MOST suitable for provisioning and managing the resources required for this use case?

1. Use Amazon EC2 Auto Scaling to deploy instances in multiple subnets
2. Use AWS CloudFormation to deploy a Cluster Placement Group on EC2
3. Use AWS Batch to deploy a multi-node parallel job
4. Use AWS Elastic Beanstalk to provision and manage the EC2 instances

Answer: 3

Explanation:

AWS Batch Multi-node parallel jobs enable you to run single jobs that span multiple Amazon EC2 instances. With AWS Batch multi-node parallel jobs, you can run large-scale, tightly coupled, high performance computing applications and distributed GPU

model training without the need to launch, configure, and manage Amazon EC2 resources directly.

An AWS Batch multi-node parallel job is compatible with any framework that supports IP-based, internode communication, such as Apache MXNet, TensorFlow, Caffe2, or Message Passing Interface (MPI).

This is the most efficient approach to deploy the resources required and supports the application requirements most effectively.

CORRECT: "Use AWS Batch to deploy a multi-node parallel job" is the correct answer.

INCORRECT: "Use Amazon EC2 Auto Scaling to deploy instances in multiple subnets" is incorrect. This is not the best solution for a tightly-coupled HPC workload with specific requirements such as MPI support.

INCORRECT: "Use AWS CloudFormation to deploy a Cluster Placement Group on EC2" is incorrect. This would deploy a cluster placement group but not manage it. AWS Batch is a better fit for large scale workloads such as this.

INCORRECT: "Use AWS Elastic Beanstalk to provision and manage the EC2 instances" is incorrect. You can certainly provision and manage EC2 instances with Elastic Beanstalk but this scenario is for a specific workload that requires MPI support and managing a HPC deployment across a large number of nodes. AWS Batch is more suitable.

References:

<https://d1.awsstatic.com/whitepapers/architecture/AWS-HPC-Lens.pdf>

<https://docs.aws.amazon.com/batch/latest/userguide/multi-node-parallel-jobs.html>

QUESTION 14

A Solutions Architect is designing an application that will run on an Amazon EC2 instance. The application must asynchronously invoke an AWS Lambda function to analyze thousands of .CSV files. The services should be decoupled.

Which service can be used to decouple the compute services?

1. Amazon SWF
2. Amazon SNS
3. Amazon Kinesis
4. Amazon OpsWorks

Answer:

Explanation:

You can use a Lambda function to process Amazon Simple Notification Service notifications. Amazon SNS supports Lambda functions as a target for messages sent to a topic. This solution decouples the Amazon EC2 application from Lambda and ensures the Lambda function is invoked.

CORRECT: "Amazon SNS" is the correct answer.

INCORRECT: "Amazon SWF" is incorrect. The Simple Workflow Service (SWF) is used for process automation. It is not well suited to this requirement.

INCORRECT: "Amazon Kinesis" is incorrect as this service is used for ingesting and processing real time streaming data, it is not a suitable service to be used solely for invoking a Lambda function.

INCORRECT: "Amazon OpsWorks" is incorrect as this service is used for configuration management of systems using Chef or Puppet.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

QUESTION 15

A large MongoDB database running on-premises must be migrated to Amazon DynamoDB within the next few weeks. The database is too large to migrate over the company's limited internet bandwidth so an alternative solution must be used. What should a Solutions Architect recommend?

1. Setup an AWS Direct Connect and migrate the database to Amazon DynamoDB using the AWS Database Migration Service (DMS)
2. Use the Schema Conversion Tool (SCT) to extract and load the data to an AWS Snowball Edge device. Use the AWS Database Migration Service (DMS) to migrate the data to Amazon DynamoDB
3. Enable compression on the MongoDB database and use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon DynamoDB
4. Use the AWS Database Migration Service (DMS) to extract and load the data to an AWS Snowball Edge device. Complete the migration to Amazon DynamoDB using AWS DMS in the AWS Cloud

Answer: 2

Explanation:

Larger data migrations with AWS DMS can include many terabytes of information. This process can be cumbersome due to network bandwidth limits or just the sheer amount of data. AWS DMS can use Snowball Edge and Amazon S3 to migrate large databases more quickly than by other methods.

When you're using an Edge device, the data migration process has the following stages:

1. You use the AWS Schema Conversion Tool (AWS SCT) to extract the data locally and move it to an Edge device.
2. You ship the Edge device or devices back to AWS.
3. After AWS receives your shipment, the Edge device automatically loads its data into an Amazon S3 bucket.
4. AWS DMS takes the files and migrates the data to the target data store. If you are using change data capture (CDC), those updates are written to the Amazon S3 bucket and then applied to the target data store.

CORRECT: "Use the Schema Conversion Tool (SCT) to extract and load the data to an AWS Snowball Edge device. Use the AWS Database Migration Service (DMS) to migrate the data to Amazon DynamoDB" is the correct answer.

INCORRECT: "Setup an AWS Direct Connect and migrate the database to Amazon DynamoDB using the AWS Database Migration Service (DMS)" is incorrect as Direct Connect connections can take several weeks to implement.

INCORRECT: "Enable compression on the MongoDB database and use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon DynamoDB" is incorrect. It's unlikely that compression is going to make the difference and the company want to avoid the internet link as stated in the scenario.

INCORRECT: "Use the AWS Database Migration Service (DMS) to extract and load the data to an AWS Snowball Edge device. Complete the migration to Amazon DynamoDB using AWS DMS in the AWS Cloud" is incorrect. This is the wrong method, the Solutions Architect should use the SCT to extract and load to Snowball Edge and then AWS DMS in the AWS Cloud.

References:

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.html

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.DynamoDB.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-database-migration-service/>

QUESTION 16

Every time an item in an Amazon DynamoDB table is modified a record must be retained for compliance reasons. What is the most efficient solution to recording this information?

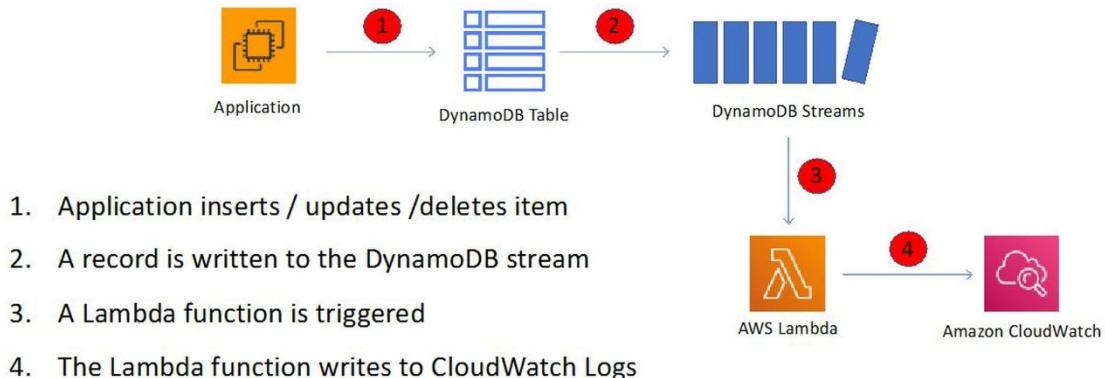
1. Enable Amazon CloudWatch Logs. Configure an AWS Lambda function to monitor the log files and record deleted item data to an Amazon S3 bucket
2. Enable DynamoDB Streams. Configure an AWS Lambda function to poll the stream and record the modified item data to an Amazon S3 bucket
3. Enable Amazon CloudTrail. Configure an Amazon EC2 instance to monitor activity in the CloudTrail log files and record changed items in another DynamoDB table
4. Enable DynamoDB Global Tables. Enable DynamoDB streams on the multi-region table and save the output directly to an Amazon S3 bucket

Answer: 2

Explanation:

Amazon DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and stores this information in a log for up to 24 hours. Applications can access this log and view the data items as they appeared before and after they were modified, in near-real time.

For example, in the diagram below a DynamoDB stream is being consumed by a Lambda function which processes the item data and records a record in CloudWatch Logs



CORRECT: "Enable DynamoDB Streams. Configure an AWS Lambda function to poll the stream and record the modified item data to an Amazon S3 bucket" is the correct answer.

INCORRECT: "Enable Amazon CloudWatch Logs. Configure an AWS Lambda function to monitor the log files and record deleted item data to an Amazon S3 bucket" is incorrect. The deleted item data will not be recorded in CloudWatch Logs.

INCORRECT: "Enable Amazon CloudTrail. Configure an Amazon EC2 instance to monitor activity in the CloudTrail log files and record changed items in another DynamoDB table" is incorrect. CloudTrail records API actions so it will not record the data from the item that was modified.

INCORRECT: "Enable DynamoDB Global Tables. Enable DynamoDB streams on the multi-region table and save the output directly to an Amazon S3 bucket" is incorrect. Global Tables is used for creating a multi-region, multi-master database. It is of no additional value for this requirement as you could just enable DynamoDB streams on the main table. You also cannot save modified data straight to an S3 bucket.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

QUESTION 17

An application in a private subnet needs to query data in an Amazon DynamoDB table. Use of the DynamoDB public endpoints must be avoided. What is the most EFFICIENT and secure method of enabling access to the table?

1. Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)
2. Create a gateway VPC endpoint and add an entry to the route table
3. Create a private Amazon DynamoDB endpoint and connect to it using an AWS VPN
4. Create a software VPN between DynamoDB and the application in the private subnet

Answer: 2

Explanation:

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

With a gateway endpoint you configure your route table to point to the endpoint. Amazon S3 and DynamoDB use gateway endpoints.

The table below helps you to understand the key differences between the two different types of VPC endpoint:

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

CORRECT: "Create a gateway VPC endpoint and add an entry to the route table" is the correct answer.

INCORRECT: "Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)" is incorrect. This would be used for services that are supported by interface endpoints, not gateway endpoints.

INCORRECT: "Create a private Amazon DynamoDB endpoint and connect to it using an AWS VPN" is incorrect. You cannot create an Amazon DynamoDB private endpoint and connect to it over VPN. Private endpoints are VPC endpoints and are connected to by instances in subnets via route table entries or via ENIs (depending on which service).

INCORRECT: "Create a software VPN between DynamoDB and the application in the private subnet" is incorrect. You cannot create a software VPN between DynamoDB and an application.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 18

A Solutions Architect needs to select a low-cost, short-term option for adding resilience to an AWS Direct Connect connection. What is the MOST cost-effective solution to provide a backup for the Direct Connect connection?

1. Implement a second AWS Direct Connection
2. Implement an IPSec VPN connection and use the same BGP prefix
3. Configure AWS Transit Gateway with an IPSec VPN backup
4. Configure an IPSec VPN connection over the Direct Connect link

Answer: 2

Explanation:

This is the most cost-effective solution. With this option both the Direct Connect connection and IPSec VPN are active and being advertised using the Border Gateway Protocol (BGP). The Direct Connect link will always be preferred unless it is unavailable.

CORRECT: "Implement an IPSec VPN connection and use the same BGP prefix" is the correct answer.

INCORRECT: "Implement a second AWS Direct Connection" is incorrect. This is not a short-term or low-cost option as it takes time to implement and is costly.

INCORRECT: "Configure AWS Transit Gateway with an IPSec VPN backup" is incorrect. This is a workable solution and provides some advantages. However, you do need to pay for the Transit Gateway so it is not the most cost-effective option and probably not suitable for a short-term need.

INCORRECT: "Configure an IPSec VPN connection over the Direct Connect link" is incorrect. This is not a solution to the problem

as the VPN connection is going over the Direct Connect link. This is something you might do to add encryption to Direct Connect but it doesn't make it more resilient.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/configure-vpn-backup-dx/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

QUESTION 19

The disk configuration for an Amazon EC2 instance must be finalized. The instance will be running an application that requires heavy read/write IOPS. A single volume is required that is 500 GiB in size and needs to support 20,000 IOPS.

What EBS volume type should be selected?

1. EBS General Purpose SSD
2. EBS Provisioned IOPS SSD
3. EBS General Purpose SSD in a RAID 1 configuration
4. EBS Throughput Optimized HDD

Answer: 2

Explanation:

This is simply about understanding the performance characteristics of the different EBS volume types. The only EBS volume type that supports over 16,000 IOPS per volume is Provisioned IOPS SSD.

SSD, General Purpose – gp2

- Volume size 1 GiB – 16 TiB.
- Max IOPS/volume 16,000.

SSD, Provisioned IOPS – i01

- Volume size 4 GiB – 16 TiB.
- Max IOPS/volume 64,000.

HDD, Throughput Optimized – (st1)

- Volume size 500 GiB – 16 TiB.

Throughput measured in MB/s, and includes the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume.

HDD, Cold – (sc1)

- Volume size 500 GiB – 16 TiB.

Lowest cost storage – cannot be a boot volume.

– These volumes can burst up to 80 MB/s per TB, with a baseline throughput of 12 MB/s per TB and a maximum throughput of 250 MB/s per volume

HDD, Magnetic – Standard – cheap, infrequently accessed storage – lowest cost storage that can be a boot volume.

CORRECT: "EBS Provisioned IOPS SSD" is the correct answer.

INCORRECT: "EBS General Purpose SSD" is incorrect as the max IOPS is 16,000.

INCORRECT: "EBS General Purpose SSD in a RAID 1 configuration" is incorrect. RAID 1 is mirroring and does not increase the amount of IOPS you can generate.

INCORRECT: "EBS Throughput Optimized HDD" is incorrect as this type of disk does not support the IOPS requirement.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 20

A new application you are designing will store data in an Amazon Aurora MySQL DB. You are looking for a way to enable inter-region disaster recovery capabilities with fast replication and fast failover. Which of the following options is the BEST solution?

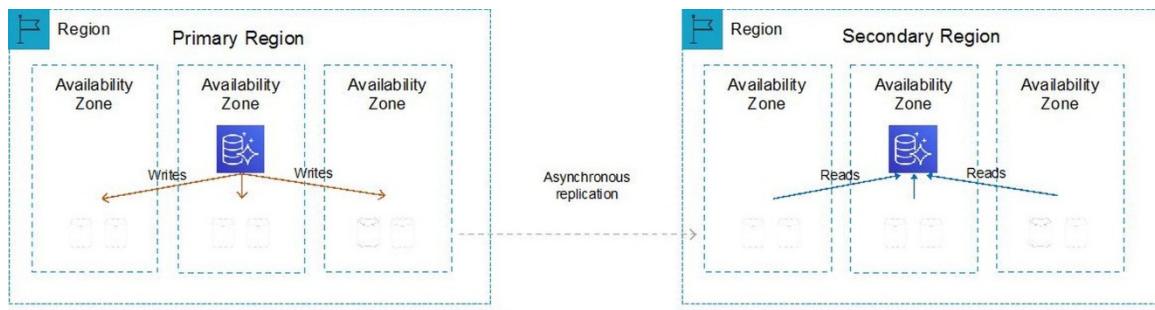
1. Use Amazon Aurora Global Database
2. Enable Multi-AZ for the Aurora DB
3. Create an EBS backup of the Aurora volumes and use cross-region replication to copy the snapshot
4. Create a cross-region Aurora Read Replica

Answer: 1

Explanation:

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages.

Aurora Global Database uses storage-based replication with typical latency of less than 1 second, using dedicated infrastructure that leaves your database fully available to serve application workloads. In the unlikely event of a regional degradation or outage, one of the secondary regions can be promoted to full read/write capabilities in less than 1 minute.



Aurora Global Database:

- Uses physical replication
- One secondary AWS region
- Uses dedicated infrastructure
- No impact on DB performance
- Good for disaster recovery

CORRECT: "Use Amazon Aurora Global Database" is the correct answer.

INCORRECT: "Enable Multi-AZ for the Aurora DB" is incorrect. Enabling Multi-AZ for the Aurora DB would provide AZ-level resiliency within the region not across regions.

INCORRECT: "Create an EBS backup of the Aurora volumes and use cross-region replication to copy the snapshot" is incorrect. Though you can take a DB snapshot and replicate it across regions, it does not provide an automated solution and it would not enable fast failover.

INCORRECT: "Create a cross-region Aurora Read Replica" is incorrect. This solution would not provide the fast storage replication and fast failover capabilities of the Aurora Global Database and is therefore not the best option.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Aurora.Replication.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 21

A Solutions Architect regularly launches EC2 instances manually from the console and wants to streamline the process to reduce administrative overhead. Which feature of EC2 enables storing of settings such as AMI ID, instance type, key pairs and Security Groups?

1. Placement Groups
2. Launch Templates
3. Run Command
4. Launch Configurations

Answer: 2

Explanation:

Launch templates enable you to store launch parameters so that you do not have to specify them every time you launch an instance. When you launch an instance using the Amazon EC2 console, an AWS SDK, or a command line tool, you can specify the launch template to use.

CORRECT: "Launch Templates" is the correct answer.

INCORRECT: "Placement Groups" is incorrect. You can launch or start instances in a *placement group*, which determines how instances are placed on underlying hardware.

INCORRECT: "Run Command" is incorrect. Run Command automates common administrative tasks, and lets you perform ad hoc configuration changes at scale.

INCORRECT: "Launch Configurations" is incorrect. Launch Configurations are used with Auto Scaling Groups.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-templates.html>

Save time with our exam-specific cheat sheets:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-templates.html>

QUESTION 22

You recently noticed that your Network Load Balancer (NLB) in one of your VPCs is not distributing traffic evenly between EC2 instances in your AZs. There are an odd number of EC2 instances spread across two AZs. The NLB is configured with a TCP listener on port 80 and is using active health checks.

What is the most likely problem?

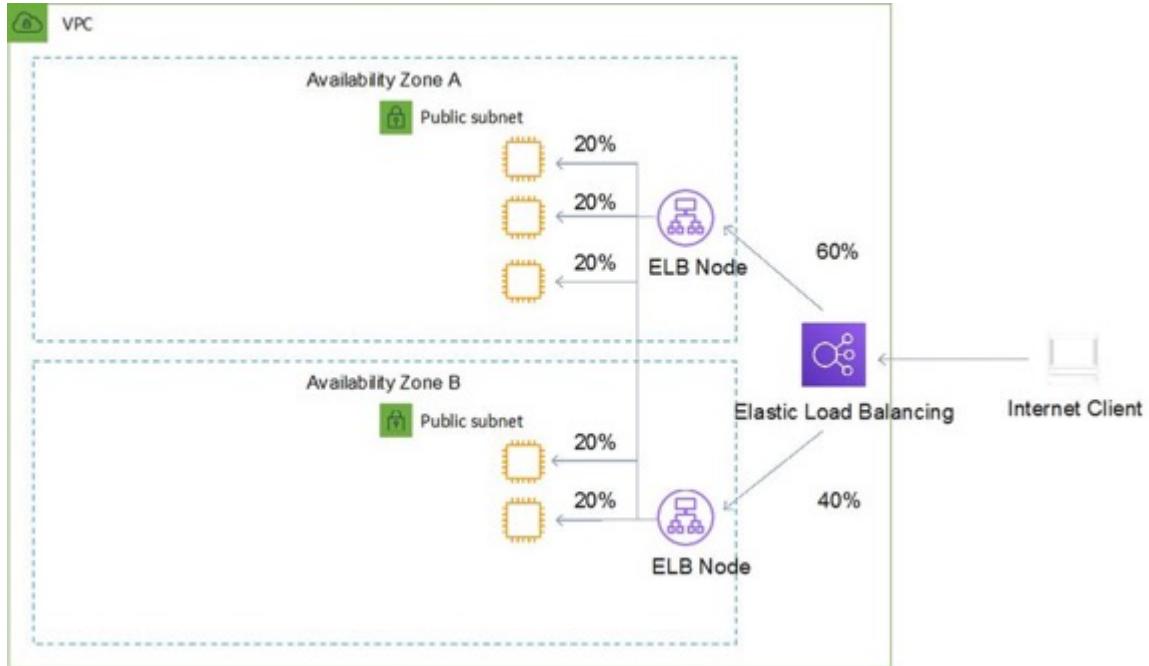
1. There is no HTTP listener
2. Health checks are failing in one AZ due to latency
3. NLB can only load balance within a single AZ
4. Cross-zone load balancing is disabled

Answer: 4

Explanation:

Without cross-zone load balancing enabled, the NLB will distribute traffic 50/50 between AZs. As there are an odd number of instances across the two AZs some instances will not receive any traffic. Therefore enabling cross-zone load balancing will ensure traffic is distributed evenly between available instances in all AZs.

The diagram below shows an ELB with cross-zone load balancing enabled:



CORRECT: "Cross-zone load balancing is disabled" is the correct answer.

INCORRECT: "There is no HTTP listener" is incorrect. Listeners are used to receive incoming connections. An NLB listens on TCP not on HTTP therefore having no HTTP listener is not the issue here.

INCORRECT: "Health checks are failing in one AZ due to latency" is incorrect. If health checks fail this will cause the NLB to stop sending traffic to these instances. However, the health check packets are very small and it is unlikely that latency would be the issue within a region.

INCORRECT: "NLB can only load balance within a single AZ" is incorrect. An NLB can load balance across multiple AZs just like the other ELB types.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 23

A Solutions Architect is creating a design for a multi-tiered serverless application. Which two services form the application facing services from the AWS serverless infrastructure? (Select TWO.)

1. API Gateway
2. AWS Cognito
3. AWS Lambda
4. Amazon ECS
5. Elastic Load Balancer

Answer: 1,3

Explanation:

The only application services here are API Gateway and Lambda and these are considered to be serverless services.

CORRECT: "API Gateway" is a correct answer.

CORRECT: "AWS Lambda" is also a correct answer.

INCORRECT: "AWS Cognito" is incorrect. AWS Cognito is used for providing authentication services for web and mobile apps.

INCORRECT: "Amazon ECS" is incorrect. ECS provides the platform for running containers and uses Amazon EC2 instances.

INCORRECT: "Elastic Load Balancer" is incorrect. ELB provides distribution of incoming network connections and also uses Amazon EC2 instances.

References:

<https://aws.amazon.com/serverless/>

Save time with our exam-specific cheat sheets:

<https://aws.amazon.com/serverless/>

QUESTION 24

A Solutions Architect attempted to restart a stopped EC2 instance and it immediately changed from a pending state to a terminated state. What are the most likely explanations? (Select TWO.)

1. You've reached your EBS volume limit
2. An EBS snapshot is corrupt
3. AWS does not currently have enough available On-Demand capacity to service your request
4. You have reached the limit on the number of instances that you can launch in a region
5. The AMI is unsupported

Answer: 1,2

Explanation:

The following are a few reasons why an instance might immediately terminate:

- You've reached your EBS volume limit.
- An EBS snapshot is corrupt.
- The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.
- The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file).

CORRECT: "You've reached your EBS volume limit" is a correct answer.

CORRECT: "An EBS snapshot is corrupt" is also a correct answer.

INCORRECT: "AWS does not currently have enough available On-Demand capacity to service your request" is incorrect. If AWS does not have capacity available a **InsufficientInstanceCapacity** error will be generated when you try to launch a new instance or restart a stopped instance.

INCORRECT: "You have reached the limit on the number of instances that you can launch in a region" is incorrect. If you've reached the limit on the number of instances you can launch in a region you get an **InstanceLimitExceeded** error when you try to launch a new instance or restart a stopped instance.

INCORRECT: "The AMI is unsupported" is incorrect. It is possible that an instance type is not supported by an AMI and this can cause an "UnsupportedOperation" client error. However, in this case the instance was previously running (it is in a stopped state) so it is unlikely that this is the issue.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 25

One of the applications you manage on RDS uses the MySQL DB and has been suffering from performance issues. You would like to setup a reporting process that will perform queries on the database but you're concerned that the extra load will further impact the performance of the DB and may lead to poor customer experience.

What would be the best course of action to take so you can implement the reporting process?

1. Configure Multi-AZ to setup a secondary database instance in another region
2. Deploy a Read Replica to setup a secondary read-only database instance
3. Deploy a Read Replica to setup a secondary read and write database instance

4. Configure Multi-AZ to setup a secondary database instance in another Availability Zone

Answer: 2

Explanation:

The reporting process will perform queries on the database but not writes. Therefore you can use a read replica which will provide a secondary read-only database and configure the reporting process to use the read replica.

Multi-AZ is used for implementing fault tolerance. With Multi-AZ you can failover to a DB in another AZ within the region in the event of a failure of the primary DB. However, you can only read and write to the primary DB so still need a read replica to offload the reporting job

CORRECT: "Deploy a Read Replica to setup a secondary read-only database instance" is the correct answer.

INCORRECT: "Configure Multi-AZ to setup a secondary database instance in another region" is incorrect as described above.

INCORRECT: "Deploy a Read Replica to setup a secondary read and write database instance" is incorrect. Read replicas are for workload offloading only and do not provide the ability to write to the database.

INCORRECT: "Configure Multi-AZ to setup a secondary database instance in another Availability Zone" is incorrect as described above.

References:

<https://aws.amazon.com/rds/features/read-replicas/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 26

A Solutions Architect is building a new Amazon Elastic Container Service (ECS) cluster. The ECS instances are running the EC2 launch type and load balancing is required to distribute connections to the tasks. It is required that the mapping of ports is performed dynamically and connections are routed to different groups of servers based on the path in the URL.

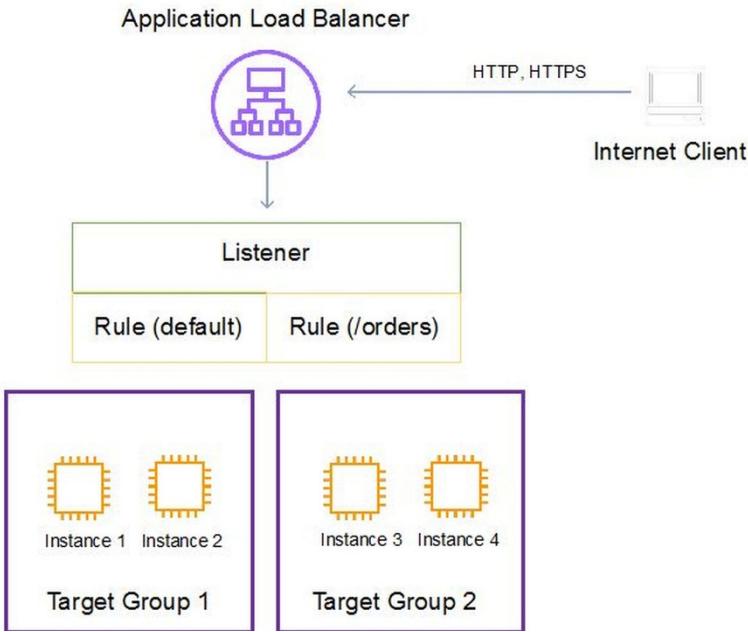
Which AWS service should the Solutions Architect choose to fulfil these requirements?

1. An Amazon ECS Service
2. Application Load Balancer
3. Network Load Balancer
4. Classic Load Balancer

Answer: 2

Explanation:

An ALB allows containers to use dynamic host port mapping so that multiple tasks from the same service are allowed on the same container host. An ALB can also route requests based on the content of the request in the host field: host-based or path-based.



The NLB and CLB types of Elastic Load Balancer do not support path-based routing or host-based routing so they cannot be used for this use case.

CORRECT: "Application Load Balancer" is the correct answer.

INCORRECT: "ECS Services" is incorrect. An Amazon ECS service enables you to run and maintain a specified number of instances of a task definition simultaneously in an Amazon ECS cluster. It does not distributed connections to tasks.

INCORRECT: "Network Load Balancer" is incorrect as described above.

INCORRECT: "Classic Load Balancer" is incorrect as described above.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/dynamic-port-mapping-ecs/>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 27

A Solutions Architect needs to connect from an office location to a Linux instance that is running in a public subnet in an Amazon VPC using the Internet. Which of the following items are required to enable this access? (Select TWO.)

1. A bastion host
2. A NAT Gateway
3. A Public or Elastic IP address on the EC2 instance
4. An Internet Gateway attached to the VPC and route table attached to the public subnet pointing to it
5. An IPSec VPN

Answer: 3,4

Explanation:

A public subnet is a subnet that has an Internet Gateway attached and "Enable auto-assign public IPv4 address" enabled. Instances require a public IP or Elastic IP address. It is also necessary to have the subnet route table updated to point to the Internet Gateway and security groups and network ACLs must be configured to allow the SSH traffic on port 22.

CORRECT: "A Public or Elastic IP address on the EC2 instance" is a correct answer.

CORRECT: "An Internet Gateway attached to the VPC and route table attached to the public subnet pointing to it" is also a

correct answer.

INCORRECT: "A bastion host" is incorrect. A bastion host can be used to access instances in private subnets but is not required for instances in public subnets.

INCORRECT: "A NAT Gateway" is incorrect. A NAT Gateway allows instances in private subnets to access the Internet, it is not used for remote access.

INCORRECT: "An IPSec VPN" is incorrect. An IPSec VPN is not required to connect to an instance in a public subnet.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstances.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 28

An Auto Scaling Group is unable to respond quickly enough to load changes resulting in lost messages from another application tier. The messages are typically around 128KB in size.

What is the best design option to prevent the messages from being lost?

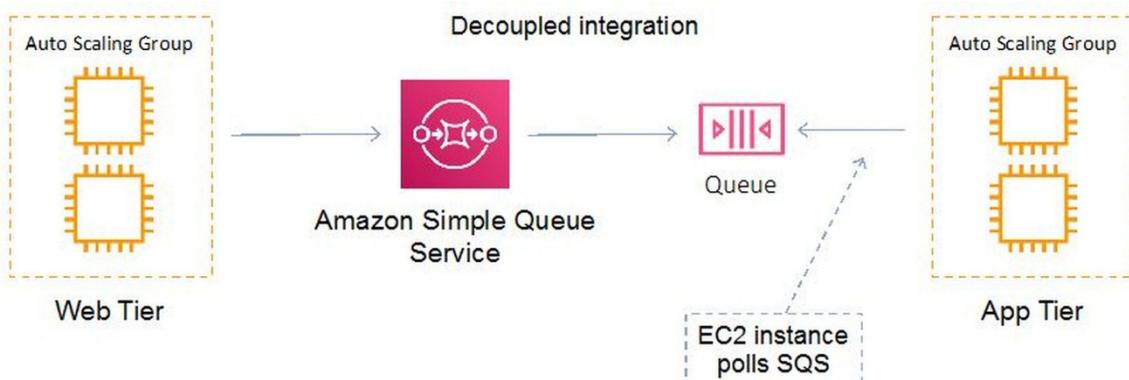
1. Store the messages on Amazon S3
2. Launch an Elastic Load Balancer
3. Store the messages on an SQS queue
4. Use larger EC2 instance sizes

Answer: 3

Explanation:

In this circumstance the ASG cannot launch EC2 instances fast enough. You need to be able to store the messages somewhere so they don't get lost whilst the EC2 instances are launched. This is a classic use case for decoupling and SQS is designed for exactly this purpose.

Amazon Simple Queue Service (Amazon SQS) is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers. An SQS queue can be used to create distributed/decoupled applications.



CORRECT: "Store the messages on an SQS queue" is the correct answer.

INCORRECT: "Store the messages on Amazon S3" is incorrect. Storing the messages on S3 is potentially feasible but SQS is the preferred solution as it is designed for decoupling. If the messages are over 256KB and therefore cannot be stored in SQS, you may want to consider using S3 and it can be used in combination with SQS by using the Amazon SQS Extended Client Library for Java.

INCORRECT: "Launch an Elastic Load Balancer" is incorrect. An ELB can help to distribute incoming connections to the back-end EC2 instances however if the ASG is not scaling fast enough then there aren't enough resources for the ELB to distribute traffic to.

INCORRECT: "Use larger EC2 instance sizes" is incorrect. Scaling horizontally and decoupling will have a greater effect over using larger instance sizes.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDriverGuide/welcome.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 29

A Solutions Architect needs to run a production batch process quickly that will use several EC2 instances. The process cannot be interrupted and must be completed within a short time period.

What is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Reserved instances
2. Spot instances
3. Flexible instances
4. On-demand instances

Answer: 4

Explanation:

The key requirements here are that you need to deploy several EC2 instances quickly to run the batch process and you must ensure that the job completes. The on-demand pricing model is the best for this ad-hoc requirement as though spot pricing may be cheaper you cannot afford to risk that the instances are terminated by AWS when the market price increases.

CORRECT: "On-demand instances" is the correct answer.

INCORRECT: "Reserved instances" is incorrect. Reserved instances are used for longer more stable requirements where you can get a discount for a fixed 1 or 3 year term. This pricing model is not good for temporary requirements.

INCORRECT: "Spot instances" is incorrect. Spot instances provide a very low hourly compute cost and are good when you have flexible start and end times. They are often used for use cases such as grid computing and high-performance computing (HPC).

INCORRECT: "Flexible instances" is incorrect. There is no such thing as a "flexible instance".

References:

<https://aws.amazon.com/ec2/pricing/>

Save time with our exam-specific cheat sheets:

References:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 30

A Solutions Architect would like to implement a method of automating the creation, retention, and deletion of backups for the Amazon EBS volumes in an Amazon VPC. What is the easiest way to automate these tasks using AWS tools?

1. Configure EBS volume replication to create a backup on Amazon S3
2. Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes
3. Create a scheduled job and run the AWS CLI command "create-backup" to take backups of the EBS volumes
4. Create a scheduled job and run the AWS CLI command "create-snapshot" to take backups of the EBS volumes

Answer: 2

Explanation:

You backup EBS volumes by taking snapshots. This can be automated via the AWS CLI command "create-snapshot". However the question is asking for a way to automate not just the creation of the snapshot but the retention and deletion too.

The EBS Data Lifecycle Manager (DLM) can automate all of these actions for you and this can be performed centrally from within the management console.

CORRECT: "Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes" is the correct answer.

INCORRECT: "Configure EBS volume replication to create a backup on S3" is incorrect. You cannot configure volume replication

for EBS volumes using AWS tools.

INCORRECT: "Create a scheduled job and run the AWS CLI command "create-backup" to take backups of the EBS volumes" is incorrect. This is the wrong command (use create-snapshot) and is not the easiest method.

INCORRECT: "Create a scheduled job and run the AWS CLI command "create-snapshot" to take backups of the EBS volumes" is incorrect. This is not the easiest method, DLM would be a much better solution.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>

<https://docs.aws.amazon.com/cli/latest/reference/ec2/create-snapshot.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 31

A mobile app uploads usage information to a database. Amazon Cognito is being used for authentication, authorization and user management and users sign-in with Facebook IDs.

In order to securely store data in DynamoDB, the design should use temporary AWS credentials. What feature of Amazon Cognito is used to obtain temporary credentials to access AWS services?

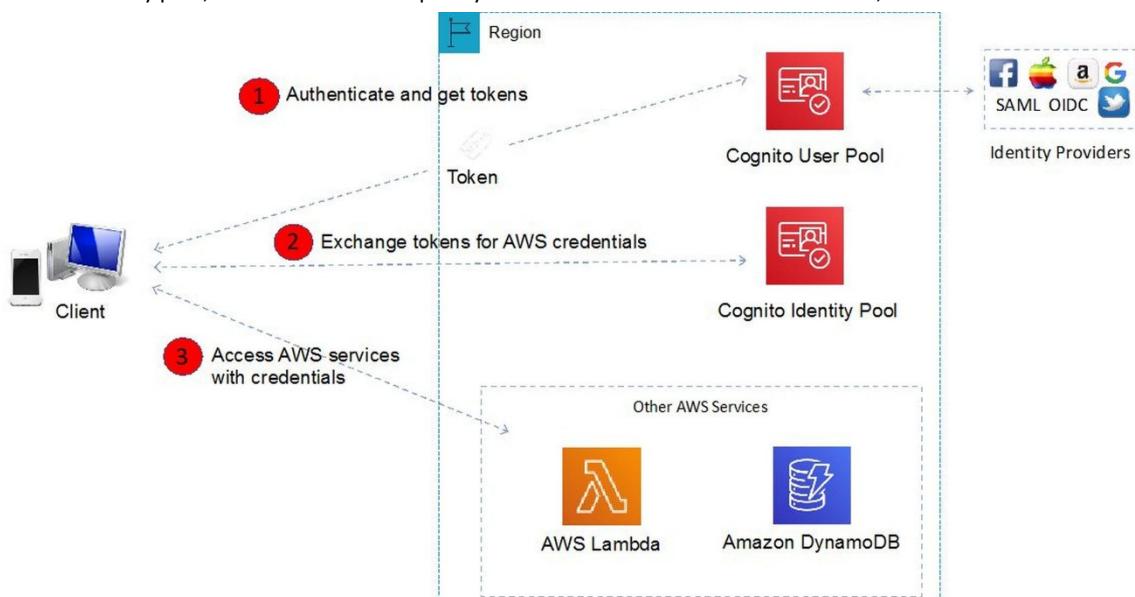
1. User Pools
2. Identity Pools
3. Key Pairs
4. SAML Identity Providers

Answer: 2

Explanation:

Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account.

With an identity pool, users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB.



CORRECT: "Identity Pools" is the correct answer.

INCORRECT: "User Pools" is incorrect. A user pool is a user directory in Amazon Cognito. With a user pool, users can sign in to web or mobile apps through Amazon Cognito, or federate through a third-party identity provider (IdP).

INCORRECT: "Key Pairs" is incorrect. Key pairs are used in Amazon EC2 for access to instances.

INCORRECT: "SAML Identity Providers" is incorrect. SAML Identity Providers are supported IDPs for identity pools but cannot be used for gaining temporary credentials for AWS services.

References:

<https://docs.aws.amazon.com/cognito/latest/developerguide/identity-pools.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 32

A website uses web servers behind an Internet-facing Elastic Load Balancer. What record set should be created to point the customer's DNS zone apex record at the ELB?

1. Create a PTR record pointing to the DNS name of the load balancer
2. Create an A record pointing to the DNS name of the load balancer
3. Create a CNAME record that is an Alias, and select the ELB DNS as a target
4. Create an A record that is an Alias, and select the ELB DNS as a target

Answer: 4

Explanation:

An Alias record can be used for resolving apex or naked domain names (e.g. example.com). You can create an A record that is an Alias that uses the customer's website zone apex domain name and map it to the ELB DNS name.

CORRECT: "Create an A record that is an Alias, and select the ELB DNS as a target" is the correct answer.

INCORRECT: "Create a PTR record pointing to the DNS name of the load balancer" is incorrect. PTR records are reverse lookup records where you use the IP to find the DNS name.

INCORRECT: "Create an A record pointing to the DNS name of the load balancer" is incorrect. A standard A record maps the DNS domain name to the IP address of a resource. You cannot obtain the IP of the ELB so you must use an Alias record which maps the DNS domain name of the customer's website to the ELB DNS name (rather than its IP).

INCORRECT: "Create a CNAME record that is an Alias, and select the ELB DNS as a target" is incorrect. A CNAME record can't be used for resolving apex or naked domain names.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/ResourceRecordTypes.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

QUESTION 33

A Solutions Architect has been assigned the task of moving some sensitive documents into the AWS cloud. The security of the documents must be maintained.

Which AWS features can help ensure that the sensitive documents cannot be read even if they are compromised? (Select TWO.)

1. AWS IAM Access Policy
2. Amazon S3 Server-Side Encryption
3. Amazon EBS snapshots
4. Amazon S3 cross region replication
5. Amazon EBS encryption with Customer Managed Keys

Answer: 2,5

Explanation:

It is not specified what types of documents are being moved into the cloud or what services they will be placed on. Therefore we can assume that options include S3 and EBS. To prevent the documents from being read if they are compromised we need to encrypt them.

Both of these services provide native encryption functionality to ensure security of the sensitive documents. With EBS you can

use KMS-managed or customer-managed encryption keys. With S3 you can use client-side or server-side encryption.

CORRECT: "Amazon S3 Server-Side Encryption" is a correct answer.

CORRECT: "Amazon EBS encryption with Customer Managed Keys" is also a correct answer.

INCORRECT: "AWS IAM Access Policy" is incorrect. IAM access policies can be used to control access but if the documents are somehow compromised they will not stop the documents from being read. For this we need encryption, and IAM access policies are not used for controlling encryption.

INCORRECT: "Amazon EBS snapshots" is incorrect. EBS snapshots are used for creating a point-in-time backup or data. They do maintain the encryption status of the data from the EBS volume but are not used for actually encrypting the data in the first place.

INCORRECT: "Amazon S3 cross region replication" is incorrect. S3 cross-region replication can be used for fault tolerance but does not apply any additional security to the data.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 34

A membership website has become quite popular and is gaining members quickly. The website currently runs on Amazon EC2 instances with one web server instance and one database instance running MySQL. A Solutions Architect is concerned about the lack of high-availability in the current architecture.

What can the Solutions Architect do to easily enable high availability without making major changes to the architecture?

1. Create a Read Replica in another availability zone
2. Enable Multi-AZ for the MySQL instance
3. Install MySQL on an EC2 instance in the same availability zone and enable replication
4. Install MySQL on an EC2 instance in another availability zone and enable replication

Answer: 4

Explanation:

If you are installing MySQL on an EC2 instance you cannot enable read replicas or multi-AZ. Instead you would need to use Amazon RDS with a MySQL DB engine to use these features.

In this example a good solution is to use the native HA features of MySQL. You would want to place the second MySQL DB instance in another AZ to enable high availability and fault tolerance.

Migrating to Amazon RDS may be a good solution but is not presented as an option.

CORRECT: "Install MySQL on an EC2 instance in another availability zone and enable replication" is the correct answer.

INCORRECT: "Create a Read Replica in another availability zone" is incorrect as described above.

INCORRECT: "Enable Multi-AZ for the MySQL instance" is incorrect as described above.

INCORRECT: "Install MySQL on an EC2 instance in the same availability zone and enable replication" is incorrect as described above.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 35

A Solutions Architect has setup a VPC with a public subnet and a VPN-only subnet. The public subnet is associated with a custom route table that has a route to an Internet Gateway. The VPN-only subnet is associated with the main route table and has a route to a virtual private gateway.

The Architect has created a new subnet in the VPC and launched an EC2 instance in it. However, the instance cannot connect to the Internet. What is the MOST likely reason?

1. The subnet has been automatically associated with the main route table which does not have a route to the Internet
2. The new subnet has not been associated with a route table
3. The Internet Gateway is experiencing connectivity problems
4. There is no NAT Gateway available in the new subnet so Internet connectivity is not possible

Answer: 1

Explanation:

When you create a new subnet, it is automatically associated with the main route table. Therefore, the EC2 instance will not have a route to the Internet. The Architect should associate the new subnet with the custom route table.

CORRECT: "The subnet has been automatically associated with the main route table which does not have a route to the Internet" is the correct answer.

INCORRECT: "The new subnet has not been associated with a route table" is incorrect. Subnets are always associated to a route table when created..

INCORRECT: "The Internet Gateway is experiencing connectivity problems" is incorrect. Internet Gateways are highly-available so it's unlikely that IGW connectivity is the issue.

INCORRECT: "There is no NAT Gateway available in the new subnet so Internet connectivity is not possible" is incorrect. NAT Gateways are used for connecting EC2 instances in private subnets to the Internet. This is a valid reason for a private subnet to not have connectivity, however in this case the Architect is attempting to use an Internet Gateway.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 36

A customer has a public-facing web application hosted on a single Amazon Elastic Compute Cloud (EC2) instance serving videos directly from an Amazon S3 bucket. Which of the following will restrict third parties from directly accessing the video assets in the bucket?

1. Launch the website Amazon EC2 instance using an IAM role that is authorized to access the videos
2. Restrict access to the bucket to the public CIDR range of the company locations
3. Use a bucket policy to only allow referrals from the main website URL
4. Use a bucket policy to only allow the public IP address of the Amazon EC2 instance hosting the customer website

Answer: 3

Explanation:

To allow read access to the S3 video assets from the public-facing web application, you can add a bucket policy that allows s3:GetObject permission with a condition, using the aws:referer key, that the get request must originate from specific webpages. This is a good answer as it fully satisfies the objective of ensuring the that EC2 instance can access the videos but direct access to the videos from other sources is prevented.

CORRECT: "Use a bucket policy to only allow referrals from the main website URL" is the correct answer.

INCORRECT: "Launch the website Amazon EC2 instance using an IAM role that is authorized to access the videos" is incorrect. Launching the EC2 instance with an IAM role that is authorized to access the videos is only half a solution as you would also need to create a bucket policy that specifies that the IAM role is granted access.

INCORRECT: "Restrict access to the bucket to the public CIDR range of the company locations" is incorrect. Restricting access to

the bucket to the public CIDR range of the company locations will stop third-parties from accessing the bucket however it will also stop the EC2 instance from accessing the bucket and the question states that the EC2 instance is serving the files directly.

INCORRECT: "Use a bucket policy to only allow the public IP address of the Amazon EC2 instance hosting the customer website" is incorrect. You can use condition statements in a bucket policy to restrict access via IP address. However, using the referrer condition in a bucket policy is preferable as it is a best practice to use DNS names / URLs instead of hard-coding IPs whenever possible.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html#example-bucket-policies-use-case-4>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 37

A Solutions Architect is creating an AWS CloudFormation template that will provision a new EC2 instance and new EBS volume. What must be specified to associate the block store with the instance?

1. Both the EC2 physical ID and the EBS physical ID
2. The EC2 physical ID
3. Both the EC2 logical ID and the EBS logical ID
4. The EC2 logical ID

Answer: 3

Explanation:

The logical ID is used to reference the resource in parts of the template. For example, if you want to map an Amazon Elastic Block Store volume to an Amazon EC2 instance, you reference the logical IDs to associate the block stores with the instance.

In addition to the logical ID, certain resources also have a physical ID, which is the actual assigned name for that resource, such as an EC2 instance ID or an S3 bucket name. Use the physical IDs to identify resources outside of AWS CloudFormation templates, but only after the resources have been created.

Think of logical IDs as being used to reference resources within the template and Physical IDs being used to identify resources outside of AWS CloudFormation templates after they have been created.

CORRECT: "Both the EC2 logical ID and the EBS logical ID" is the correct answer.

INCORRECT: "Both the EC2 physical ID and the EBS physical ID" is incorrect as logical IDs can be used within the template.

INCORRECT: "The EC2 physical ID" is incorrect as logical IDs can be used.

INCORRECT: "The EC2 logical ID" is incorrect as the EBS logical ID should also be specified.

References:

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

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/>

QUESTION 38

An application stores encrypted data in Amazon S3 buckets. A Solutions Architect needs to be able to query the encrypted data using SQL queries and write the encrypted results back to the S3 bucket. As the data is sensitive fine-grained control must be implemented over access to the S3 bucket.

What combination of services represent the BEST options support these requirements? (Select TWO.)

1. Use AWS Glue to extract the data, analyze it, and load it back to the S3 bucket
2. Use bucket ACLs to restrict access to the bucket
3. Use IAM policies to restrict access to the bucket
4. Use Athena for querying the data and writing the results back to the bucket
5. Use the AWS KMS API to query the encrypted data, and the S3 API for writing the results

Answer: 3,4

Explanation:

Athena allows you to easily query encrypted data stored in Amazon S3 and write encrypted results back to your S3 bucket. Both, server-side encryption and client-side encryption are supported.

AWS IAM policies can be used to grant IAM users' with fine-grained control to Amazon S3 buckets.

CORRECT: "Use IAM policies to restrict access to the bucket" is a correct answer.

CORRECT: "Use Athena for querying the data and writing the results back to the bucket" is also a correct answer.

INCORRECT: "Use AWS Glue to extract the data, analyze it, and load it back to the S3 bucket" is incorrect. AWS Glue is an ETL service and is not used for querying and analyzing data in S3.

INCORRECT: "Use bucket ACLs to restrict access to the bucket" is incorrect. With IAM policies, you can grant IAM users fine-grained control to your S3 buckets, and is preferable to using bucket ACLs.

INCORRECT: "Use the AWS KMS API to query the encrypted data, and the S3 API for writing the results" is incorrect. The AWS KMS API can be used for encryption purposes, however it cannot perform analytics so is not suitable.

References:

<https://aws.amazon.com/athena/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 39

A Solutions Architect works for a systems integrator running a platform that stores medical records. The government security policy mandates that patient data that contains personally identifiable information (PII) must be encrypted at all times, both at rest and in transit. Amazon S3 is used to back up data into the AWS cloud.

How can the Solutions Architect ensure the medical records are properly secured? (Select TWO.)

1. Before uploading the data to S3 over HTTPS, encrypt the data locally using your own encryption keys
2. Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-128
3. Attach an encrypted EBS volume to an EC2 instance
4. Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-256
5. Upload the data using CloudFront with an EC2 origin

Answer: 1,4

Explanation:

When data is stored in an encrypted state it is referred to as encrypted "at rest" and when it is encrypted as it is being transferred over a network it is referred to as encrypted "in transit". You can securely upload/download your data to Amazon S3 via SSL endpoints using the HTTPS protocol (In Transit – SSL/TLS).

You have the option of encrypting the data locally before it is uploaded or uploading using SSL/TLS so it is secure in transit and encrypting on the Amazon S3 side using S3 managed keys. The S3 managed keys will be AES-256 (not AES-128) bit keys

Uploading data using CloudFront with an EC2 origin or using an encrypted EBS volume attached to an EC2 instance is not a solution to this problem as your company wants to backup these records onto S3 (not EC2/EBS).

CORRECT: "Before uploading the data to S3 over HTTPS, encrypt the data locally using your own encryption keys" is a correct answer.

CORRECT: "Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-256" is also a correct answer.

INCORRECT: "Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-128" is incorrect as AES 256 should be used.

INCORRECT: "Attach an encrypted EBS volume to an EC2 instance" is incorrect as explained above.

INCORRECT: "Upload the data using CloudFront with an EC2 origin" is incorrect as explained above.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

Save time with our exam-specific cheat sheets:

QUESTION 40

A Solutions Architect is considering the best approach to enabling Internet access for EC2 instances in a private subnet. What advantages do NAT Gateways have over NAT Instances? (Select TWO.)

1. Can be assigned to security groups
2. Can be used as a bastion host
3. Managed for you by AWS
4. Highly available within each AZ
5. Can be scaled up manually

Answer: 3,4

Explanation:

NAT gateways are managed for you by AWS. NAT gateways are highly available in each AZ into which they are deployed. They are not associated with any security groups and can scale automatically up to 45Gbps

NAT instances are managed by you. They must be scaled manually and do not provide HA. NAT Instances can be used as bastion hosts and can be assigned to security groups.

NAT Instance	NAT Gateway
Managed by you (e.g. software updates)	Managed by AWS
Scale up (instance type) manually and use enhanced networking	Elastic scalability up to 45 Gbps
No high availability – scripted/auto-scaled HA possible using multiple NATs in multiple subnets	Provides automatic high availability within an AZ and can be placed in multiple AZs
Need to assign Security Group	No Security Groups
Can use as a bastion host	Cannot access through SSH
Use an Elastic IP address or a public IP address with a NAT instance	Choose the Elastic IP address to associate with a NAT gateway at creation
Can implement port forwarding through manual customisation	Does not support port forwarding

CORRECT: "Managed for you by AWS" is a correct answer.

CORRECT: "Highly available within each AZ" is also a correct answer.

INCORRECT: "Can be assigned to security groups" is incorrect as you cannot assign security groups to NAT gateways but you can to NAT instances.

INCORRECT: "Can be used as a bastion host" is incorrect, only a NAT instance can be used as a bastion host.

INCORRECT: "Can be scaled up manually" is incorrect, though automatic is better anyway!

References:

QUESTION 41

A Solutions Architect must design a solution for providing single sign-on to existing staff in a company. The staff manage on-premise web applications and also need access to the AWS management console to manage resources in the AWS cloud.

Which combination of services are BEST suited to delivering these requirements?

1. Use IAM and Amazon Cognito
2. Use your on-premise LDAP directory with IAM
3. Use the AWS Secure Token Service (STS) and SAML
4. Use IAM and MFA

Answer: 3

Explanation:

Single sign-on using federation allows users to login to the AWS console without assigning IAM credentials. The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (such as federated users from an on-premise directory).

Federation (typically Active Directory) uses SAML 2.0 for authentication and grants temporary access based on the users AD credentials. The user does not need to be a user in IAM.

CORRECT: "Use the AWS Secure Token Service (STS) and SAML" is the correct answer.

INCORRECT: "Use IAM and Amazon Cognito" is incorrect. Amazon Cognito is used for authenticating users to web and mobile apps not for providing single sign-on between on-premises directories and the AWS management console.

INCORRECT: "Use your on-premise LDAP directory with IAM" is incorrect. You cannot use your on-premise LDAP directory with IAM, you must use federation.

INCORRECT: "Use IAM and MFA" is incorrect. Enabling multi-factor authentication (MFA) for IAM is not a federation solution..

References:

<https://aws.amazon.com/identity/federation/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 42

A Solutions Architect is designing a three-tier web application that includes an Auto Scaling group of Amazon EC2 Instances running behind an Elastic Load Balancer. The security team requires that all web servers must be accessible only through the Elastic Load Balancer and that none of the web servers are directly accessible from the Internet.

How should the Architect meet these requirements?

1. Create an Amazon CloudFront distribution in front of the Elastic Load Balancer
2. Configure the web servers' security group to deny traffic from the Internet
3. Configure the web tier security group to allow only traffic from the Elastic Load Balancer
4. Install a Load Balancer on an Amazon EC2 instance

Answer: 3

Explanation:

The web servers must be kept private so they will not have public IP addresses. The ELB is Internet-facing so it will be publicly accessible via its DNS address (and corresponding public IP).

To restrict web servers to be accessible only through the ELB you can configure the web tier security group to allow only traffic from the ELB. You would normally do this by adding the ELBs security group to the rule on the web tier security group

CORRECT: "Configure the web tier security group to allow only traffic from the Elastic Load Balancer" is the correct answer.

INCORRECT: "Create an Amazon CloudFront distribution in front of the Elastic Load Balancer" is incorrect. CloudFront distributions are used for caching content to improve performance for users on the Internet. They are not security devices to be used for restricting access to EC2 instances.

INCORRECT: "Configure the web servers' security group to deny traffic from the Internet" is incorrect. You cannot create deny rules in security groups.

INCORRECT: "Install a Load Balancer on an Amazon EC2 instance" is incorrect. This scenario is using an Elastic Load Balancer and these cannot be installed on EC2 instances (at least not by you, in reality all ELBs are actually running on EC2 instances but these are transparent to the AWS end user).

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-update-security-groups.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 43

A Solutions Architect is creating a URL that lets users who sign in to the organization's network securely access the AWS Management Console. The URL will include a sign-in token that authenticates the user to AWS. Microsoft Active Directory Federation Services is being used as the identity provider (IdP).

Which of the steps below will the Solutions Architect need to include when developing the custom identity broker? (Select TWO.)

1. Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token
2. Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
3. Assume an IAM Role through the console or programmatically with the AWS CLI, Tools for Windows PowerShell or API
4. Generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET
5. Delegate access to the IdP through the "Configure Provider" wizard in the IAM console

Answer: 1,2

Explanation:

The aim of this solution is to create a single sign-on solution that enables users signed in to the organization's Active Directory service to be able to connect to AWS resources. When developing a custom identity broker you use the AWS STS service.

The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users). The steps performed by the custom identity broker to sign users into the AWS management console are:

- Verify that the user is authenticated by your local identity system
- Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
- Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token
- Construct a URL for the console that includes the token
- Give the URL to the user or invoke the URL on the user's behalf

CORRECT: "Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token" is the correct answer.

CORRECT: "Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user" is the correct answer.

INCORRECT: "Assume an IAM Role through the console or programmatically with the AWS CLI, Tools for Windows PowerShell or API" is incorrect as this is an example of federation so assuming a role is the wrong procedure.

INCORRECT: "Generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET" is incorrect. You cannot generate a pre-signed URL for this purpose using SDKs, delegate access through the IAM console or directly assume IAM roles..

INCORRECT: "Delegate access to the IdP through the "Configure Provider" wizard in the IAM console" is incorrect as this is not something you can do

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-custom-url.html

Save time with our exam-specific cheat sheets:

QUESTION 44

Some Amazon ECS containers are running on a cluster using the EC2 launch type. The current configuration uses the container instance's IAM roles for assigning permissions to the containerized applications.

A Solutions Architect needs to implement more granular permissions so that some applications can be assigned more restrictive permissions. How can this be achieved?

1. This cannot be changed as IAM roles can only be linked to container instances
2. This can be achieved using IAM roles for tasks, and splitting the containers according to the permissions required to different task definition profiles
3. This can be achieved by configuring a resource-based policy for each application
4. This can only be achieved using the Fargate launch type

Answer: 2

Explanation:

With IAM roles for Amazon ECS tasks, you can specify an IAM role that can be used by the containers in a task. Using this feature you can achieve the required outcome by using IAM roles for tasks and splitting the containers according to the permissions required to different task profiles.

CORRECT: "This can be achieved using IAM roles for tasks, and splitting the containers according to the permissions required to different task definition profiles" is the correct answer.

INCORRECT: "This cannot be changed as IAM roles can only be linked to container instances" is incorrect as you can also link them to tasks.

INCORRECT: "This can be achieved by configuring a resource-based policy for each application" is incorrect. Amazon ECS does not support IAM resource-based policies.

INCORRECT: "This can only be achieved using the Fargate launch type" is incorrect. The solution can be achieved whether using the EC2 or Fargate launch types.

References:

<https://docs.aws.amazon.com/AmazonECS/latest/ug/task-iam-roles.html>

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

QUESTION 45

An application uses a combination of Reserved and On-Demand instances to handle typical load. The application involves performing analytics on a set of data. A Solutions Architect needs to temporarily deploy a large number of EC2 instances. The instances must be available for a short period of time until the analytics job is completed.

If job completion is not time-critical, what is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

1. Use Spot instances
2. Use dedicated hosts
3. Use On-Demand instances
4. Use Reserved instances

Answer: 1

Explanation:

The key requirements here are that you need to temporarily deploy a large number of instances, can tolerate an delay (not time-critical), and need the most economical solution. In this case Spot instances are likely to be the most economical solution.

You must be able to tolerate delays if using Spot instances as if the market price increases your instances will be terminated and you may have to wait for the price to lower back to your budgeted allowance.

CORRECT: "Use Spot instances" is the correct answer.

INCORRECT: "Use dedicated hosts" is incorrect. An EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. They are much more expensive than on-demand or Spot instances and are used for use cases such as bringing your own socket-based software licences to AWS or for compliance reasons.

INCORRECT: "Use On-Demand instances" is incorrect. On-demand is good for temporary deployments when you cannot tolerate any delays (instances being terminated by AWS). It is likely to be more expensive than Spot however so if delays can be tolerated it is not the best solution.

INCORRECT: "Use Reserved instances" is incorrect. Reserved instances are used for longer more stable requirements where you can get a discount for a fixed 1 or 3 year term. This pricing model is not good for temporary requirements.

References:

<https://aws.amazon.com/ec2/pricing/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 46

There is a problem with an EC2 instance that was launched by Amazon EC2 Auto Scaling. The EC2 status checks have reported that the instance is "Impaired". What action will EC2 Auto Scaling take?

1. Auto Scaling will perform Availability Zone rebalancing
2. It will wait a few minutes for the instance to recover and if it does not it will mark the instance for termination, terminate it, and then launch a replacement
3. Auto Scaling performs its own status checks and does not integrate with EC2 status checks
4. It will launch a new instance immediately and then mark the impaired one for replacement

Answer: 2

Explanation:

If any health check returns an unhealthy status the instance will be terminated. For the "impaired" status, the ASG will wait a few minutes to see if the instance recovers before taking action. If the "impaired" status persists, termination occurs. Unlike AZ rebalancing, termination of unhealthy instances happens first, then Auto Scaling attempts to launch new instances to replace terminated instances.

CORRECT: "It will wait a few minutes for the instance to recover and if it does not it will mark the instance for termination, terminate it, and then launch a replacement" is the correct answer.

INCORRECT: "Auto Scaling will perform Availability Zone rebalancing" is incorrect. Auto Scaling will not perform Availability Zone rebalancing due to an impaired status check.

INCORRECT: "Auto Scaling performs its own status checks and does not integrate with EC2 status checks" is incorrect. Auto Scaling does integrate with EC2 status checks as well as having its own status checks.

INCORRECT: "It will launch a new instance immediately and then mark the impaired one for replacement" is incorrect. Auto Scaling will not launch a new instance immediately as it always terminates unhealthy instance before launching a replacement.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/auto-scaling-terminate-instance/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 47

A pharmaceutical company uses a strict process for release automation that involves building and testing services in 3 separate VPCs. A peering topology is configured with VPC-A peered with VPC-B and VPC-B peered with VPC-C. The development team wants to modify the process so that they can release code directly from VPC-A to VPC-C.

How can this be accomplished?

1. Update VPC-Bs route table with peering targets for VPC-A and VPC-C and enable route propagation
2. Create a new VPC peering connection between VPC-A and VPC-C
3. Update the CIDR blocks to match to enable inter-VPC routing

4. Update VPC-As route table with an entry using the VPC peering as a target

Answer: 2

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network.

You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

It is not possible to use transitive peering relationships with VPC peering and therefore you must create an additional VPC peering connection between VPC-A and VPC-C.

CORRECT: "Create a new VPC peering connection between VPC-A and VPC-C" is the correct answer.

INCORRECT: "Update VPC-Bs route table with peering targets for VPC-A and VPC-C and enable route propagation" is incorrect. Route propagation cannot be used to extend VPC peering connections.

INCORRECT: "Update the CIDR blocks to match to enable inter-VPC routing" is incorrect. You cannot have matching (overlapping) CIDR blocks with VPC peering.

INCORRECT: "Update VPC-As route table with an entry using the VPC peering as a target" is incorrect. You must update route tables to configure routing however updating VPC-As route table alone will not lead to the desired result without first creating the additional peering connection.

References:

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 48

A Solutions Architect needs to work programmatically with IAM. Which feature of IAM allows direct access to the IAM web service using HTTPS to call service actions and what is the method of authentication that must be used? (Select TWO.)

1. OpenID Connect
2. Query API
3. API Gateway
4. Access key ID and secret access key
5. IAM role

Answer: 2,4

Explanation:

AWS recommend that you use the AWS SDKs to make programmatic API calls to IAM. However, you can also use the IAM Query API to make direct calls to the IAM web service. An access key ID and secret access key must be used for authentication when using the Query API.

CORRECT: "Query API" is a correct answer.

CORRECT: "Access key ID and secret access key" is also a correct answer.

INCORRECT: "OpenID Connect" is incorrect. OpenID Connect is a provider for connecting external directories.

INCORRECT: "API Gateway" is incorrect. API gateway is a separate service for accepting and processing API calls.

INCORRECT: "IAM role" is incorrect. An IAM role is not used for authentication to the Query API.

References:

<https://docs.aws.amazon.com/IAM/latest/APIReference/iam-api.pdf>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 49

The Systems Administrators in a company currently use Chef for configuration management of on-premise servers. Which AWS service can a Solutions Architect use that will provide a fully-managed configuration management service that will enable the use of existing Chef cookbooks?

1. Elastic Beanstalk
2. CloudFormation
3. OpsWorks for Chef Automate
4. Opsworks Stacks

Answer: 3

Explanation:

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. AWS OpsWorks for Chef Automate is a fully-managed configuration management service that hosts Chef Automate, a suite of automation tools from Chef for configuration management, compliance and security, and continuous deployment. OpsWorks for Chef Automate is completely compatible with tooling and cookbooks from the Chef community and automatically registers new nodes with your Chef server.

CORRECT: "OpsWorks for Chef Automate" is the correct answer.

INCORRECT: "Opsworks Stacks" is incorrect. AWS OpsWorks Stacks lets you manage applications and servers on AWS and on-premises and uses Chef Solo. The question does not require the managed solution on AWS to manage on-premises resources, just to use existing cookbooks so this is not the preferred solution.

INCORRECT: "Elastic Beanstalk" is incorrect. AWS Elastic Beanstalk is not able to build infrastructure using Chef cookbooks.

INCORRECT: "CloudFormation" is incorrect. AWS CloudFormation is not able to build infrastructure using Chef cookbooks.

References:

<https://aws.amazon.com/opsworks/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-opsworks/>

QUESTION 50

An Amazon RDS Multi-AZ deployment is running in an Amazon VPC. An outage occurs in the availability zone of the primary RDS database instance. What actions will take place in this circumstance? (Select TWO.)

1. The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance
2. A failover will take place once the connection draining timer has expired
3. A manual failover of the DB instance will need to be initiated using Reboot with failover
4. The primary DB instance will switch over automatically to the standby replica
5. Due to the loss of network connectivity the process to switch to the standby replica cannot take place

Answer: 1,4

Explanation:

Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it (DR only).

A failover may be triggered in the following circumstances:

- Loss of primary AZ or primary DB instance failure
- Loss of network connectivity on primary
- Compute (EC2) unit failure on primary
- Storage (EBS) unit failure on primary
- The primary DB instance is changed
- Patching of the OS on the primary DB instance
- Manual failover (reboot with failover selected on primary)

During failover RDS automatically updates configuration (including DNS endpoint) to use the second node.

CORRECT: "The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance" is a correct answer.

CORRECT: "The primary DB instance will switch over automatically to the standby replica" is also a correct answer.

INCORRECT: "A failover will take place once the connection draining timer has expired" is incorrect. Connection draining timers are applicable to ELBs not RDS.

INCORRECT: "A manual failover of the DB instance will need to be initiated using Reboot with failover" is incorrect. You do not need to manually failover the DB instance, multi-AZ has an automatic process as outlined above.

INCORRECT: "Due to the loss of network connectivity the process to switch to the standby replica cannot take place" is incorrect. The process to failover is not reliant on network connectivity as it is designed for fault tolerance.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 51

A Solutions Architect is designing a web-facing application. The application will run on Amazon EC2 instances behind Elastic Load Balancers in multiple regions in an active/passive configuration. The website address the application runs on is example.com. AWS Route 53 will be used to perform DNS resolution for the application.

How should the Solutions Architect configure AWS Route 53 in this scenario based on AWS best practices? (Select TWO.)

1. Use a Failover Routing Policy
2. Set Evaluate Target Health to "No" for the primary
3. Use a Weighted Routing Policy
4. Connect the ELBs using Alias records
5. Connect the ELBs using CNAME records

Answer: 1,4

Explanation:

The failover routing policy is used for active/passive configurations. Alias records can be used to map the domain apex (example.com) to the Elastic Load Balancers.

Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. The primary and secondary records can route traffic to anything from an Amazon S3 bucket that is configured as a website to a complex tree of records.

CORRECT: "Use a Failover Routing Policy" is a correct answer.

CORRECT: "Connect the ELBs using Alias records" is also a correct answer.

INCORRECT: "Set Evaluate Target Health to "No" for the primary" is incorrect. For Evaluate Target Health choose Yes for your primary record and choose No for your secondary record. For your primary record choose Yes for Associate with Health Check. Then for Health Check to Associate select the health check that you created for your primary resource.

INCORRECT: "Use a Weighted Routing Policy" is incorrect. Weighted routing is not an active/passive routing policy. All records are active and the traffic is distributed according to the weighting.

INCORRECT: "Connect the ELBs using CNAME records" is incorrect. You cannot use CNAME records for the domain apex record, you must use Alias records.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-failover>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

QUESTION 52

A Solutions Architect is designing a new retail website for a high-profile company. The company has previously been the victim of targeted distributed denial-of-service (DDoS) attacks and has requested that the design includes mitigation techniques.

Which of the following are the BEST techniques to help ensure the availability of the services is not compromised in an attack? (Select TWO.)

1. Configure Auto Scaling with a high maximum number of instances to ensure it can scale accordingly
2. Use CloudFront for distributing both static and dynamic content
3. Use Spot instances to reduce the cost impact in case of attack
4. Use encryption on your EBS volumes
5. Use Placement Groups to ensure high bandwidth and low latency

Answer: 1,2

Explanation:

CloudFront distributes traffic across multiple edge locations and filters requests to ensure that only valid HTTP(S) requests will be forwarded to backend hosts. CloudFront also supports geoblocking, which you can use to prevent requests from particular geographic locations from being served.

Auto Scaling helps to maintain a desired count of EC2 instances running at all times and setting a high maximum number of instances allows your fleet to grow and absorb some of the impact of the attack.

CORRECT: "Configure Auto Scaling with a high maximum number of instances to ensure it can scale accordingly" is a correct answer.

CORRECT: "Use CloudFront for distributing both static and dynamic content" is also a correct answer.

INCORRECT: "Use Spot instances to reduce the cost impact in case of attack" is incorrect. Spot instances may reduce the cost (depending on the current Spot price) however the question asks us to focus on availability not cost.

INCORRECT: "Use encryption on your EBS volumes" is incorrect. Encrypting EBS volumes does not help in a DDoS attack as the attack is targeted at reducing availability rather than compromising data.

INCORRECT: "Use Placement Groups to ensure high bandwidth and low latency" is incorrect as this will not assist with mitigation of DDoS attacks.

References:

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

<https://docs.aws.amazon.com/waf/latest/developerguide/tutorials-ddos-cross-service.html>

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 53

An application running on Amazon EC2 requires an EBS volume for saving structured data. The application vendor suggests that the performance of the disk should be up to 3 IOPS per GB. The capacity is expected to grow to 2 TB.

Taking into account cost effectiveness, which EBS volume type should be used?

1. Throughput Optimized HDD (ST1)
2. General Purpose (GP2)
3. Provisioned IOPS (Io1)
4. Cold HDD (SC1)

Answer: 2

Explanation:

SSD, General Purpose (GP2) provides enough IOPS to support this requirement and is the most economical option that does. Using Provisioned IOPS would be more expensive and the other two options do not provide an SLA for IOPS.

More information on the volume types:

- SSD, General Purpose (GP2) provides 3 IOPS per GB up to 16,000 IOPS. Volume size is 1 GB to 16 TB.
- Provisioned IOPS (Io1) provides the IOPS you assign up to 50 IOPS per GiB and up to 64,000 IOPS per volume. Volume size is 4 GB to 16TB.

– Throughput Optimized HDD (ST1) provides up to 500 IOPS per volume but does not provide an SLA for IOPS.

– Cold HDD (SC1) provides up to 250 IOPS per volume but does not provide an SLA for IOPS.

CORRECT: "General Purpose (GP2)" is the correct answer.

INCORRECT: "Throughput Optimized HDD (ST1)" is incorrect as this will not provide an SLA for IOPS.

INCORRECT: "Provisioned IOPS (Io1)" is incorrect as this will be less cost-effective.

INCORRECT: "Cold HDD (SC1)" is incorrect as this will not provide an SLA for IOPS.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html?icmpid=docs_ec2_console

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 54

An application in an Amazon VPC uses an Auto Scaling Group that spans 3 AZs and there are currently 4 Amazon EC2 instances running in the group. What actions will Auto Scaling take, by default, if it needs to terminate an EC2 instance?

1. Randomly select one of the 3 AZs, and then terminate an instance in that AZ
2. Terminate the instance with the least active network connections. If multiple instances meet this criterion, one will be randomly selected
3. Send an SNS notification, if configured to do so
4. Wait for the cooldown period and then terminate the instance that has been running the longest
5. Terminate an instance in the AZ which currently has 2 running EC2 instances

Answer: 3,5

Explanation:

Auto Scaling can perform rebalancing when it finds that the number of instances across AZs is not balanced. Auto Scaling rebalances by launching new EC2 instances in the AZs that have fewer instances first, only then will it start terminating instances in AZs that had more instances

Auto Scaling can be configured to send an SNS email when:

- An instance is launched.
- An instance is terminated.
- An instance fails to launch.
- An instance fails to terminate.

CORRECT: "Send an SNS notification, if configured to do so" is a correct answer.

CORRECT: "Terminate an instance in the AZ which currently has 2 running EC2 instances" is also a correct answer.

INCORRECT: "Terminate the instance with the least active network connections. If multiple instances meet this criterion, one will be randomly selected" is incorrect. Auto Scaling will only terminate an instance randomly after it has first gone through several other selection steps. Please see the AWS article below for detailed information on the process

INCORRECT: "Wait for the cooldown period and then terminate the instance that has been running the longest" is incorrect. Auto Scaling does not terminate the instance that has been running the longest.

INCORRECT: "Randomly select one of the 3 AZs, and then terminate an instance in that AZ" is incorrect as described above.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 55

Several environments are being created in a single Amazon VPC. The Solutions Architect needs to implement a system of categorization that allows for identification of Amazon EC2 resources by business unit, owner, or environment.

Which AWS feature can be used?

1. Parameters
2. Metadata
3. Custom filters
4. Tags

Answer: 4

Explanation:

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment.

CORRECT: "Tags" is the correct answer.

INCORRECT: "Parameters" is incorrect. Parameters are not used for categorization

INCORRECT: "Metadata" is incorrect. Instance metadata is data about your instance that you can use to configure or manage the running instance.

INCORRECT: "Custom filters" is incorrect. Custom filters are not used for categorization.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 56

An organization has a data lake on Amazon S3 and needs to find a solution for performing in-place queries of the data assets in the data lake. The requirement is to perform both data discovery and SQL querying, and complex queries from a large number of concurrent users using BI tools.

What is the BEST combination of AWS services to use in this situation? (Select TWO.)

1. RedShift Spectrum for the complex queries
2. Amazon Athena for the ad hoc SQL querying
3. AWS Glue for the ad hoc SQL querying
4. AWS Lambda for the complex queries
5. Amazon Kinesis for the complex queries

Answer: 1,2

Explanation:

Performing in-place queries on a data lake allows you to run sophisticated analytics queries directly on the data in S3 without having to load it into a data warehouse.

You can use both Athena and Redshift Spectrum against the same data assets. You would typically use Athena for ad hoc data discovery and SQL querying, and then use Redshift Spectrum for more complex queries and scenarios where a large number of data lake users want to run concurrent BI and reporting workloads.

CORRECT: "RedShift Spectrum for the complex queries" is a correct answer.

CORRECT: "Amazon Athena for the ad hoc SQL querying" is also a correct answer.

INCORRECT: "AWS Glue for the ad hoc SQL querying" is incorrect. AWS Glue is an extract, transform and load (ETL) service.

INCORRECT: "AWS Lambda for the complex queries" is incorrect. AWS Lambda is a serverless technology for running functions, it is not the best solution for running analytics queries.

INCORRECT: "Amazon Kinesis for the complex queries" is incorrect. Amazon Kinesis is used for ingesting and processing real time streaming data, not performing queries.

References:

<https://docs.aws.amazon.com/aws-technical-content/latest/building-data-lakes/in-place-querying.html>

<https://aws.amazon.com/redshift/>

<https://aws.amazon.com/athena/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-athena/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>

QUESTION 57

When using throttling controls with API Gateway what happens when request submissions exceed the steady-state request rate and burst limits?

1. API Gateway fails the limit-exceeding requests and returns "429 Too Many Requests" error responses to the client
2. The requests will be buffered in a cache until the load reduces
3. API Gateway drops the requests and does not return a response to the client
4. API Gateway fails the limit-exceeding requests and returns "500 Internal Server Error" error responses to the client

Answer: 1

Explanation:

You can throttle and monitor requests to protect your backend. Resiliency through throttling rules based on the number of requests per second for each HTTP method (GET, PUT). Throttling can be configured at multiple levels including Global and Service Call.

When request submissions exceed the steady-state request rate and burst limits, API Gateway fails the limit-exceeding requests and returns 429 Too Many Requests error responses to the client.

CORRECT: "API Gateway fails the limit-exceeding requests and returns "429 Too Many Requests" error responses to the client" is the correct answer.

INCORRECT: "The requests will be buffered in a cache until the load reduces" is incorrect as the requests are actually failed.

INCORRECT: "API Gateway drops the requests and does not return a response to the client" is incorrect as it does return a response as detailed above.

INCORRECT: "API Gateway fails the limit-exceeding requests and returns "500 Internal Server Error" error responses to the client" is incorrect as a 429 error is returned.

References:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/>

QUESTION 58

A Solutions Architect created a new VPC and setup an Auto Scaling Group to maintain a desired count of 2 Amazon EC2 instances. The security team has requested that the EC2 instances be located in a private subnet. To distribute load, an Internet-facing Application Load Balancer (ALB) is also required.

With the security team's requirements in mind, what else needs to be done to get this configuration to work? (Select TWO.)

1. Attach an Internet Gateway to the private subnets
2. Associate the public subnets with the ALB
3. Add an Elastic IP address to each EC2 instance in the private subnet
4. Add a NAT gateway to the private subnet
5. For each private subnet create a corresponding public subnet in the same AZ

Answer: 2,5

Explanation:

ELB nodes have public IPs and route traffic to the private IP addresses of the EC2 instances. You need one public subnet in each AZ where the ELB is defined and the private subnets are located

CORRECT: "Associate the public subnets with the ALB" is a correct answer.

CORRECT: "For each private subnet create a corresponding public subnet in the same AZ" is also a correct answer.

INCORRECT: "Attach an Internet Gateway to the private subnets" is incorrect. Attaching an Internet gateway (which is done at the VPC level, not the subnet level) or a NAT gateway will not assist as these are both used for outbound communications which is not the goal here.

INCORRECT: "Add an Elastic IP address to each EC2 instance in the private subnet" is incorrect. ELBs talk to the private IP addresses of the EC2 instances so adding an Elastic IP address to the instance won't help. Additionally Elastic IP addresses are used in public subnets to allow Internet access via an Internet Gateway.

INCORRECT: "Add a NAT gateway to the private subnet" is incorrect as this would only enable outbound internet access.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 59

An application running AWS uses an Elastic Load Balancer (ELB) to distribute connections between EC2 instances. A Solutions Architect needs to record information on the requester, IP, and request type for connections made to the ELB. Additionally, the Architect will also need to perform some analysis on the log files.

Which AWS services and configuration options can be used to collect and then analyze the logs? (Select TWO.)

1. Use EMR for analyzing the log files
2. Update the application to use DynamoDB for storing log files
3. Use Elastic Transcoder to analyze the log files
4. Enable Access Logs on the ELB and store the log files on S3
5. Enable Access Logs on the EC2 instances and store the log files on S3

Answer: 1,4

Explanation:

The best way to deliver these requirements is to enable access logs on the ELB and then use EMR for analyzing the log files. Access Logs on ELB are disabled by default. Information includes information about the clients (not included in CloudWatch metrics) such as the identity of the requester, IP, request type etc. Logs can be optionally stored and retained in S3.

Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3.

CORRECT: "Use EMR for analyzing the log files" is the correct answer.

CORRECT: "Enable Access Logs on the ELB and store the log files on S3" is the correct answer.

INCORRECT: "Update the application to use DynamoDB for storing log files" is incorrect. The information recorded by ELB access logs is exactly what you require so there is no need to get the application to record the information into DynamoDB.

INCORRECT: "Use Elastic Transcoder to analyze the log files" is incorrect. Elastic Transcoder is used for converting media file formats not analyzing files.

INCORRECT: "Enable Access Logs on the EC2 instances and store the log files on S3" is incorrect as the access logs on the ELB should be enabled.

References:

<https://aws.amazon.com/blogs/aws/access-logs-for-elastic-load-balancers/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/>

QUESTION 60

A Solutions Architect would like to store a backup of an Amazon EBS volume on Amazon S3. What is the easiest way of achieving this?

1. Use SWF to automatically create a backup of your EBS volumes and then upload them to an S3 bucket
2. You don't need to do anything, EBS volumes are automatically backed up by default
3. Write a custom script to automatically copy your data to an S3 bucket
4. Create a snapshot of the volume

Answer: 4

Explanation:

Snapshots capture a point-in-time state of an instance. Snapshots of Amazon EBS volumes are stored on S3 by design so you only need to take a snapshot and it will automatically be stored on Amazon S3.

CORRECT: "Create a snapshot of the volume" is the correct answer.

INCORRECT: "Use SWF to automatically create a backup of your EBS volumes and then upload them to an S3 bucket" is incorrect. This is not a good use case for Amazon SWF.

INCORRECT: "You don't need to do anything, EBS volumes are automatically backed up by default" is incorrect. Amazon EBS volumes are not automatically backed up using snapshots. You need to manually take a snapshot or you can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots.

INCORRECT: "Write a custom script to automatically copy your data to an S3 bucket" is incorrect as this is not the simplest solution available.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 61

An application will gather data from a website hosted on an EC2 instance and write the data to an S3 bucket. The application will use API calls to interact with the EC2 instance and S3 bucket.

Which Amazon S3 access control method will be the MOST operationally efficient? (Select TWO.)

1. Create a bucket policy
2. Grant programmatic access
3. Use key pairs
4. Grant AWS Management Console access
5. Create an IAM policy

Answer: 2,5

Explanation:

Policies are documents that define permissions and can be applied to users, groups and roles. Policy documents are written in JSON (key value pair that consists of an attribute and a value).

Within an IAM policy you can grant either programmatic access or AWS Management Console access to Amazon S3 resources.

CORRECT: "Grant programmatic access" is a correct answer.

CORRECT: "Create an IAM policy" is also a correct answer.

INCORRECT: "Create a bucket policy" is incorrect as it is more efficient to use an IAM policy.

INCORRECT: "Use key pairs" is incorrect. Key pairs are used for access to EC2 instances; a bucket policy would not assist with access control with EC2 and granting management console access will not assist the application which is making API calls to the services.

INCORRECT: "Grant AWS Management Console access" is incorrect as programmatic access is required.

References:

<https://aws.amazon.com/blogs/security/writing-iam-policies-how-to-grant-access-to-an-amazon-s3-bucket/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 62

An Amazon CloudWatch alarm recently notified a Solutions Architect that the load on an Amazon DynamoDB table is getting close to the provisioned capacity for writes. The DynamoDB table is part of a two-tier customer-facing application and is configured using provisioned capacity.

What will happen if the limit for the provisioned capacity for writes is reached?

1. The requests will be throttled, and fail with an HTTP 503 code (Service Unavailable)
2. DynamoDB scales automatically so there's no need to worry
3. The requests will be throttled, and fail with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceededException
4. The requests will succeed, and an HTTP 200 status code will be returned

Answer: 3

Explanation:

Amazon DynamoDB can throttle requests that exceed the provisioned throughput for a table. When a request is throttled it fails with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceeded exception (not a 503 or 200 status code).

When using the provisioned capacity pricing model DynamoDB does not automatically scale. DynamoDB can automatically scale when using the new on-demand capacity mode, however this is not configured for this database.

CORRECT: "The requests will be throttled, and fail with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceededException" is the correct answer.

INCORRECT: "The requests will be throttled, and fail with an HTTP 503 code (Service Unavailable)" is incorrect as this is not the code that is used (see above).

INCORRECT: "DynamoDB scales automatically so there's no need to worry" is incorrect as provisioned capacity mode does not automatically scale.

INCORRECT: "The requests will succeed, and an HTTP 200 status code will be returned" is incorrect as the request will fail as described above.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Programming.Errors.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

QUESTION 63

A Solutions Architect is creating the business process workflows associated with an order fulfilment system. What AWS service can assist with coordinating tasks across distributed application components?

1. AWS STS
2. Amazon SQS
3. Amazon SWF
4. Amazon SNS

Answer: 3

Explanation:

Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks.

CORRECT: "Amazon SWF" is the correct answer.

INCORRECT: "AWS STS" is incorrect. AWS Security Token Service (STS) is used for requesting temporary credentials.

INCORRECT: "Amazon SQS" is incorrect. Amazon Simple Queue Service (SQS) is a message queue used for decoupling application components.

INCORRECT: "Amazon SNS" is incorrect. Amazon Simple Notification Service (SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud. SNS supports notifications over multiple transports including HTTP/HTTPS, Email/Email-JSON, SQS and SMS.

References:

<https://aws.amazon.com/swf/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-swf/>

QUESTION 64

An EC2 instance in an Auto Scaling group is having some issues that are causing it to launch new instances based on the dynamic scaling policy. A Solutions Architect needs to troubleshoot the EC2 instance and prevent the Auto Scaling group from launching new instances temporarily.

What is the best method to accomplish this? (Select TWO.)

1. Remove the EC2 instance from the Target Group
2. Disable the launch configuration associated with the EC2 instance
3. Place the EC2 instance that is experiencing issues into the Standby state
4. Suspend the scaling processes responsible for launching new instances
5. Disable the dynamic scaling policy

Answer: 3,4

Explanation:

You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. This can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes. You can manually move an instance from an ASG and put it in the standby state

Instances in standby state are still managed by Auto Scaling, are charged as normal, and do not count towards available EC2 instance for workload/application use. Auto scaling does not perform health checks on instances in the standby state. Standby state can be used for performing updates/changes/troubleshooting etc. without health checks being performed or replacement instances being launched.

CORRECT: "Place the EC2 instance that is experiencing issues into the Standby state" is a correct answer.

CORRECT: "Suspend the scaling processes responsible for launching new instances" is also a correct answer.

INCORRECT: "Remove the EC2 instance from the Target Group" is incorrect. Target Groups are features of ELB (specifically ALB/NLB). Removing the instance from the target group will stop the ELB from sending connections to it but will not stop Auto Scaling from launching new instances while you are troubleshooting it.

INCORRECT: "Disable the launch configuration associated with the EC2 instance" is incorrect. You cannot disable the launch configuration and you can't modify a launch configuration after you've created it.

INCORRECT: "Disable the dynamic scaling policy" is incorrect. You do not need to disable the dynamic scaling policy, you can just suspend it as previously described.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 65

An Amazon VPC has been deployed with private and public subnets. A MySQL database server running on an Amazon EC2 instance will soon be launched. According to AWS best practice, which subnet should the database server be launched into?

1. It doesn't matter
2. The private subnet
3. The public subnet

4. The subnet that is mapped to the primary AZ in the region

Answer: 2

Explanation:

AWS best practice is to deploy databases into private subnets wherever possible. You can then deploy your web front-ends into public subnets and configure these, or an additional application tier to write data to the database.

CORRECT: "The private subnet" is the correct answer.

INCORRECT: "It doesn't matter" is incorrect as the best practice does recommend using a private subnet.

INCORRECT: "The public subnet" is incorrect. Public subnets are typically used for web front-ends as they are directly accessible from the Internet. It is preferable to launch your database in a private subnet.

INCORRECT: "The subnet that is mapped to the primary AZ in the region" is incorrect. There is no such thing as a "primary" Availability Zone (AZ). All AZs are essentially created equal and your subnets map 1:1 to a single AZ.

References:

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

SET 5: PRACTICE QUESTIONS ONLY

For training purposes, go directly to [Set 5: Practice Questions, Answers & Explanations](#)

QUESTION 1

A Solutions Architect has deployed an API using Amazon API Gateway and created usage plans and API keys for several customers. Requests from one particular customer have been excessive and the solutions architect needs to limit the rate of requests. Other customers should not be affected. How should the solutions architect proceed?

1. Configure a server-side throttling limit
2. Configure the per-method throttling limits
3. Configure per-client throttling limits
4. Configure the account-level throttling limits

QUESTION 2

A Solutions Architect is deploying a high performance computing (HPC) application on Amazon EC2 instances. The application requires extremely low inter-instance latency. How should the instances be deployed for BEST performance?

1. Use an instance with enhanced networking and deploy the instances in a partition placement group
2. Use an Elastic Fabric Adapter (EFA) and deploy instances in a cluster placement group
3. Add multiple Elastic Network Adapters (ENAs) to each instance and create a NIC team
4. Use an EBS-optimized instance with 10 Gigabit networking and deploy to a single subnet

QUESTION 3

A company has deployed an API using Amazon API Gateway. There are many repeat requests and a solutions architect has been asked to implement measures to reduce request latency and the number of calls to the Amazon EC2 endpoint.

How can this be most easily achieved?

1. Create a cache for a stage and configure a TTL
2. Create a cache for a method and configure a TTL
3. Configure an edge-optimized endpoint with CloudFront
4. Configure a private endpoint place ElastiCache in front

QUESTION 4

A Solutions Architect is designing a migration strategy for a company moving to the AWS Cloud. The company use a shared Microsoft filesystem that uses Distributed File System Namespaces (DFSN). What will be the MOST suitable migration strategy for the filesystem?

1. Use the AWS Server Migration Service to migrate to an Amazon S3 bucket
2. Use the AWS Server Migration Service to migrate to Amazon FSx for Lustre
3. Use AWS DataSync to migrate to an Amazon EFS filesystem
4. Use AWS DataSync to migrate to Amazon FSx for Windows File Server

QUESTION 5

An Amazon ElastiCache for Redis cluster runs across multiple Availability Zones. A solutions architect is concerned about the security of sensitive data as it is replicated between nodes. How can the solutions architect protect the sensitive data?

1. Issue a Redis AUTH command
2. Enable in-transit encryption
3. Enable at-rest encryption
4. Set up MFA and API logging

QUESTION 6

A company runs an application on-premises that must consume a REST API running on Amazon API Gateway. The company has an AWS Direct Connect connection to their Amazon VPC. The solutions architect wants all API calls to use private addressing

only and avoid the internet. How can this be achieved?

1. Use a transit virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway
2. Use a private virtual interface and create a VPC Endpoint for Amazon API Gateway
3. Use a hosted virtual interface and create a VPC Endpoint for Amazon API Gateway
4. Use a public virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway

QUESTION 7

A company has an eCommerce application that runs from multiple AWS Regions. Each region has a separate database running on Amazon EC2 instances. The company plans to consolidate the data to a columnar database and run analytics queries. Which approach should the company take?

1. Run an AWS Batch job to copy and process the data into a columnar Amazon RDS database. Use Amazon Athena to analyze the data
2. Use the COPY command to load data into an Amazon RedShift data warehouse and run the analytics queries there
3. Launch Amazon Kinesis Data Streams producers to load data into a Kinesis Data stream. Use Kinesis Data Analytics to analyze the data
4. Create an AWS Lambda function that copies the data onto Amazon S3. Use Amazon S3 Select to query the data

QUESTION 8

There has been an increase in traffic to an application that writes data to an Amazon DynamoDB database. Thousands of random table reads occur per second and low-latency is required. What can a Solutions Architect do to improve performance for the reads without negatively impacting the rest of the application?

1. Increase the number of Amazon DynamoDB write capacity units
2. Add an Amazon SQS queue to decouple the requests
3. Use Amazon DynamoDB Accelerator to cache the reads
4. Use an Amazon Kinesis Data Stream to decouple requests

QUESTION 9

A Solutions Architect must enable an application to download software updates from the internet. The application runs on a series of EC2 instances in an Auto Scaling group running in a private subnet. The solution must involve minimal ongoing systems management effort. How should the Solutions Architect proceed?

1. Implement a NAT gateway
2. Launch a NAT instance
3. Create a Virtual Private Gateway
4. Attach Elastic IP addresses

QUESTION 10

A Solutions Architect manages multiple Amazon RDS MySQL databases. To improve security, the Solutions Architect wants to enable secure user access with short-lived credentials. How can these requirements be met?

1. Configure the MySQL databases to use the AWS Security Token Service (STS)
2. Configure the application to use the AUTH command to send a unique password
3. Create the MySQL user accounts to use the AWSAuthenticationPlugin with IAM
4. Configure the MySQL databases to use AWS KMS data encryption keys

QUESTION 11

An application is running in a private subnet of an Amazon VPC and must have outbound internet access for downloading updates. The Solutions Architect does not want the application exposed to inbound connection attempts. Which steps should be taken?

1. Create a NAT gateway but do not attach an internet gateway to the VPC
2. Attach an internet gateway to the private subnet and create a NAT gateway

3. Attach an internet gateway to the VPC but do not create a NAT gateway
4. Create a NAT gateway and attach an internet gateway to the VPC

QUESTION 12

An application has been migrated from on-premises to an Amazon EC2 instance. The migration has failed to an unknown dependency that the application must communicate with an on-premises server using private IP addresses.

Which action should a solutions architect take to quickly provision the necessary connectivity?

1. Setup an AWS Direct Connect connection
2. Configure a Virtual Private Gateway
3. Create an Amazon CloudFront distribution
4. Create an AWS Transit Gateway

QUESTION 13

A company runs an API on a Linux server in their on-premises data center. The company are planning to migrate the API to the AWS cloud. The company require a highly available, scalable and cost-effective solution. What should a Solutions Architect recommend?

1. Migrate the API to Amazon API Gateway and migrate the backend to Amazon EC2
2. Migrate the API server to Amazon EC2 instances in an Auto Scaling group and attach an Application Load Balancer
3. Migrate the API to Amazon API Gateway and use AWS Lambda as the backend
4. Migrate the API to Amazon CloudFront and use AWS Lambda as the origin

QUESTION 14

An application that is being installed on an Amazon EC2 instance requires a persistent block storage volume. The data must be encrypted at rest and regular volume-level backups must be automated.

Which solution options should be used?

1. Use an encrypted Amazon EBS volume and use Data Lifecycle Manager to automate snapshots
2. Use an encrypted Amazon EFS filesystem and use an Amazon CloudWatch Events rule to start a backup copy of data using AWS Lambda
3. Use server-side encryption on an Amazon S3 bucket and use Cross-Region-Replication to backup on a schedule
4. Use an encrypted Amazon EC2 instance store and copy the data to another EC2 instance using a cron job and a batch script

QUESTION 15

A company has several AWS accounts each with multiple Amazon VPCs. The company must establish routing between all private subnets. The architecture should be simple and allow transitive routing to occur.

How should the network connectivity be configured?

1. Create a transitive VPC peering connection between each Amazon VPC and configure route tables
2. Create an AWS Transit Gateway and share it with each account using AWS Resource Access Manager
3. Create an AWS Managed VPN between each Amazon VPC and configure route tables
4. Create a hub-and-spoke topology with AWS App Mesh and use AWS Resource Access Manager to share route tables

QUESTION 16

An organization is planning their disaster recovery solution. They plan to run a scaled down version of a fully functional environment. In a DR situation the recovery time must be minimized.

Which DR strategy should a Solutions Architect recommend?

1. Backup and restore
2. Pilot light
3. Warm standby
4. Multi-site

QUESTION 17

An application analyzes images of people that are uploaded to an Amazon S3 bucket. The application determines demographic data which is then saved to a .CSV file in another S3 bucket. The data must be encrypted at rest and then queried using SQL. The solution should be fully serverless.

Which actions should a Solutions Architect take to encrypt and query the data?

1. Use Amazon S3 server-side encryption and use Amazon RedShift Spectrum to query the data
2. Use AWS KMS encryption keys for the S3 bucket and use Amazon Athena to query the data
3. Use AWS KMS encryption keys for the S3 bucket and use Amazon Kinesis Data Analytics to query the data
4. Use Amazon S3 server-side encryption and Amazon QuickSight to query the data

QUESTION 18

A large quantity of data is stored on a NAS device on-premises and accessed using the SMB protocol. The company require a managed service for hosting the filesystem and a tool to automate the migration.

Which actions should a Solutions Architect take?

1. Migrate the data to Amazon EFS using the AWS Server Migration Service (SMS)
2. Migrate the data to Amazon FSx for Lustre using AWS DataSync
3. Migrate the data to Amazon FSx for Windows File Server using AWS DataSync
4. Migrate the data to Amazon S3 using and AWS Snowball Edge device

QUESTION 19

The database layer of an on-premises web application is being migrated to AWS. The database uses a multi-threaded, in-memory caching layer to improve performance for repeated queries. Which service would be the most suitable replacement for the database cache?

1. Amazon ElastiCache Redis
2. Amazon DynamoDB DAX
3. Amazon ElastiCache Memcached
4. Amazon RDS MySQL

QUESTION 20

A Solutions Architect is designing an application for processing and extracting data from log files. The log files are generated by an application and the number and frequency of updates varies. The files are up to 1 GB in size and processing will take around 40 seconds for each file.

Which solution is the most cost-effective?

1. Write the log files to an Amazon EC2 instance with an attached EBS volume. After processing, save the files to an Amazon S3 bucket
2. Write the log files to an Amazon SQS queue. Use AWS Lambda to process the files from the queue and save to an Amazon S3 bucket
3. Write the log files to an Amazon S3 bucket. Create an event notification to invoke an Amazon ECS task to process the files and save to an Amazon S3 bucket
4. Write the log files to an Amazon S3 bucket. Create an event notification to invoke an AWS Lambda function that will process the files

QUESTION 21

A large multinational retail company has a presence in AWS in multiple regions. The company has established a new office and needs to implement a high-bandwidth, low-latency connection to multiple VPCs in multiple regions within the same account. The VPCs each have unique CIDR ranges.

What would be the optimum solution design using AWS technology? (Select TWO.)

1. Configure AWS VPN CloudHub
2. Create a Direct Connect gateway, and create private VIFs to each region
3. Provision an MPLS network

4. Implement Direct Connect connections to each AWS region
5. Implement a Direct Connect connection to the closest AWS region

QUESTION 22

A Solutions Architect is creating a design for a two-tier application with a MySQL RDS back-end. The performance requirements of the database tier are hard to quantify until the application is running and the Architect is concerned about right-sizing the database.

What methods of scaling are possible after the MySQL RDS database is deployed? (Select TWO.)

1. Vertical scaling for read and write by choosing a larger instance size
2. Horizontal scaling for write capacity by enabling Multi-AZ
3. Vertical scaling for read and write by using Transfer Acceleration
4. Horizontal scaling for read and write by enabling Multi-Master RDS DB
5. Horizontal scaling for read capacity by creating a read-replica

QUESTION 23

An application is running on EC2 instances in a private subnet of an Amazon VPC. A Solutions Architect would like to connect the application to Amazon API Gateway. For security reasons, it is necessary to ensure that no traffic traverses the Internet and to ensure all traffic uses private IP addresses only.

How can this be achieved?

1. Create a NAT gateway
2. Create a public VIF on a Direct Connect connection
3. Create a private API using an interface VPC endpoint
4. Add the API gateway to the subnet the EC2 instances are located in

QUESTION 24

An application stack is being created which needs a message bus to decouple the application components from each other. The application will generate up to 300 messages per second without using batching. A Solutions Architect needs to ensure that a message is delivered only once and duplicates are not introduced into the queue. It is not necessary to maintain the order of the messages.

Which SQS queue type should be used?

1. Standard queues
2. Long polling queues
3. FIFO queues
4. Auto Scaling queues

QUESTION 25

A Solutions Architect is attempting to clean up unused EBS volumes and snapshots to save some space and cost. How many of the most recent snapshots of an EBS volume need to be maintained to guarantee that you can recreate the full EBS volume from the snapshot?

1. You must retain all snapshots as the process is incremental and therefore data is required from each snapshot
2. Two snapshots, the oldest and most recent snapshots
3. The oldest snapshot, as this references data in all other snapshots
4. Only the most recent snapshot. Snapshots are incremental, but the deletion process will ensure that no data is lost

QUESTION 26

A Python application is currently running on Amazon ECS containers using the Fargate launch type. An ALB has been created with a Target Group that routes incoming connections to the ECS-based application. The application will be used by consumers who will authenticate using federated OIDC compliant Identity Providers such as Google and Facebook. The users must be securely authenticated on the front-end before they access the secured portions of the application.

How can this be configured using an ALB?

1. The only option is to use SAML with Amazon Cognito on the ALB
2. This can be done on the ALB by creating an authentication action on a listener rule that configures an Amazon Cognito user pool with the social IdP
3. This cannot be done on an ALB; you'll need to authenticate users on the back-end with AWS Single Sign-On (SSO) integration
4. This cannot be done on an ALB; you'll need to use another layer in front of the ALB

QUESTION 27

A Solutions Architect is creating a solution for an application that must be deployed on Amazon EC2 hosts that are dedicated to the client. Instance placement must be automatic and billing should be per instance.

Which type of EC2 deployment model should be used?

1. Reserved Instance
2. Dedicated Instance
3. Dedicated Host
4. Cluster Placement Group

QUESTION 28

There is new requirement for a database that will store a large number of records for an online store. You are evaluating the use of DynamoDB. Which of the following are AWS best practices for DynamoDB? (Select TWO.)

1. Use separate local secondary indexes for each item
2. Store objects larger than 400KB in S3 and use pointers in DynamoDB
3. Store more frequently and less frequently accessed data in separate tables
4. Use for BLOB data use cases
5. Use large files

QUESTION 29

A Solutions Architect needs to migrate an Oracle database running on RDS onto Amazon RedShift to improve performance and reduce cost. What combination of tasks using AWS services should be followed to execute the migration? (Select TWO.)

1. Migrate the database using the AWS Database Migration Service (DMS)
2. Convert the schema using the AWS Schema Conversion Tool
3. Take a snapshot of the Oracle database and restore the snapshot onto RedShift
4. Configure API Gateway to extract, transform and load the data into RedShift
5. Enable log shipping from the Oracle database to RedShift

QUESTION 30

A client has made some updates to their web application. The application uses an Auto Scaling Group to maintain a group of several EC2 instances. The application has been modified and a new AMI must be used for launching any new instances.

What does a Solutions Architect need to do to add the new AMI?

1. Create a new target group that uses a new launch configuration with the new AMI
2. Modify the existing launch configuration to add the new AMI
3. Suspend Auto Scaling and replace the existing AMI
4. Create a new launch configuration that uses the AMI and update the ASG to use the new launch configuration

QUESTION 31

A Solutions Architect regularly deploys and manages infrastructure services for customers on AWS. The SysOps team are facing challenges in tracking changes that are made to the infrastructure services and rolling back when problems occur.

How can a Solutions Architect BEST assist the SysOps team?

1. Use AWS Systems Manager to manage all updates to the infrastructure services
2. Use CodeDeploy to manage version control for the infrastructure services
3. Use CloudFormation templates to deploy and manage the infrastructure services
4. Use Trusted Advisor to record updates made to the infrastructure services

QUESTION 32

A Solutions Architect is designing the compute layer of a serverless application. The compute layer will manage requests from external systems, orchestrate serverless workflows, and execute the business logic.

The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the compute layer? (Select TWO.)

1. Use Amazon ECS for executing the business logic
2. Use AWS CloudFormation for orchestrating serverless workflows
3. Use AWS Step Functions for orchestrating serverless workflows
4. Use AWS Elastic Beanstalk for executing the business logic
5. Use Amazon API Gateway with AWS Lambda for executing the business logic

QUESTION 33

An application running in an on-premise data center writes data to a MySQL database. A Solutions Architect is re-architecting the application and plans to move the database layer into the AWS cloud on Amazon RDS. The application layer will run in the on-premise data center.

What must be done to connect the application to the RDS database via the Internet? (Select TWO.)

1. Configure a NAT Gateway and attach the RDS database
2. Choose to make the RDS instance publicly accessible and place it in a public subnet
3. Select a public IP within the DB subnet group to assign to the RDS instance
4. Create a security group allowing access from the on-premise public IP to the RDS instance and assign to the RDS instance
5. Create a DB subnet group that is publicly accessible

QUESTION 34

A Solutions Architect is conducting an audit and needs to query several properties of EC2 instances in a VPC. Which two methods are available for accessing and querying the properties of an EC2 instance such as instance ID, public keys and network interfaces? (Select TWO.)

1. Use the EC2 Config service
2. Run the command “curl http://169.254.169.254/latest/meta-data/”
3. Download and run the Instance Metadata Query Tool
4. Run the command “curl http://169.254.169.254/latest/dynamic/instance-identity/”
5. Use the Batch command

QUESTION 35

Encrypted Amazon Elastic Block Store (EBS) volumes are attached to some Amazon EC2 instances. Which statements are correct about using encryption with Amazon EBS volumes? (Select TWO.)

1. Data is only encrypted at rest
2. Encryption is supported on all Amazon EBS volume types
3. Data in transit between an instance and an encrypted volume is also encrypted
4. Volumes created from encrypted snapshots are unencrypted
5. You cannot mix encrypted with unencrypted volumes on an instance

QUESTION 36

An operations team would like to be notified if an RDS database exceeds certain metric thresholds. How can a Solutions Architect automate this process for the operations team?

1. Create a CloudWatch alarm and associate an SQS queue with it that delivers a message to SES
2. Setup an RDS alarm and associate an SNS topic with it that sends an email
3. Create a CloudTrail alarm and configure a notification event to send an SMS
4. Create a CloudWatch alarm and associate an SNS topic with it that sends an email notification

QUESTION 37

An Amazon VPC contains a mixture of Amazon EC2 instances in production and non-production environments. A Solutions Architect needs to devise a way to segregate access permissions to different sets of users for instances in different environments.

How can this be achieved? (Select TWO.)

1. Attach an Identity Provider (IdP) and delegate access to the instances to the relevant groups
2. Create an IAM policy that grants access to any instances with the specific tag and attach to the users and groups
3. Create an IAM policy with a conditional statement that matches the environment variables
4. Add an environment variable to the instances using user data
5. Add a specific tag to the instances you want to grant the users or groups access to

QUESTION 38

A customer runs an application on-premise that stores large media files. The data is mounted to different servers using either the SMB or NFS protocols. The customer is having issues with scaling the storage infrastructure on-premise and is looking for a way to offload the data set into the cloud whilst retaining a local cache for frequently accessed content.

Which of the following is the best solution?

1. Use the AWS Storage Gateway File Gateway
2. Use the AWS Storage Gateway Volume Gateway in cached volume mode
3. Create a script that migrates infrequently used data to S3 using multi-part upload
4. Establish a VPN and use the Elastic File System (EFS)

QUESTION 39

A client has requested a design for a fault tolerant database that can failover between AZs. You have decided to use RDS in a multi-AZ configuration. What type of replication will the primary database use to replicate to the standby instance?

1. Continuous replication
2. Asynchronous replication
3. Scheduled replication
4. Synchronous replication

QUESTION 40

A Solutions Architect needs a storage solution for a fleet of Linux web application servers. The solution should provide a file system interface and be able to support millions of files. Which AWS service should the Architect choose?

1. Amazon ElastiCache
2. Amazon EBS
3. Amazon EFS
4. Amazon S3

QUESTION 41

A Solutions Architect is creating an application design with several components that will be publicly addressable. The Architect would like to use Alias records. Using Route 53 Alias records what targets can you specify? (Select TWO.)

1. CloudFront distribution
2. ElastiCache cluster
3. EFS filesystems
4. Elastic Beanstalk environment
5. On-premise web server

QUESTION 42

A new financial platform has been re-architected to use Docker containers in a micro-services architecture. The new architecture will be implemented on AWS and a Solutions Architect must recommend the solution configuration. For operational reasons, it will be necessary to access the operating system of the instances on which the containers run.

Which solution delivery option should the Architect select?

1. ECS with the EC2 launch type
2. EKS with Kubernetes managed infrastructure
3. ECS with the Fargate launch type
4. ECS with a default cluster

QUESTION 43

A new application runs on Amazon EC2 instances and uses API Gateway and AWS Lambda. The company is planning on running an advertising campaign that will likely result in significant hits to the application after each ad is run.

A Solutions Architect is concerned about the impact this may have on the application and would like to put in place some controls to limit the number of requests per second that hit the application.

What controls should the Solutions Architect implement?

1. Implement throttling rules on the API Gateway
2. Enable caching on the API Gateway and specify a size in gigabytes
3. Enable Lambda continuous scaling
4. API Gateway and Lambda scale automatically to handle any load so there's no need to implement controls

QUESTION 44

A Solutions Architect has deployed a number of AWS resources using CloudFormation. Some changes must be made to a couple of resources within the stack. Due to recent failed updates, the Solutions Architect is a little concerned about the effects that implementing updates to the resources might have on other resources in the stack.

What is the easiest way to proceed cautiously?

1. Create and execute a change set
2. Use OpsWorks to manage the configuration changes
3. Use a direct update
4. Deploy a new stack to test the changes

QUESTION 45

A company has over 2000 users and is planning to migrate data into the AWS Cloud. Some of the data is user's home folders on an existing file share and the plan is to move this data to Amazon S3. Each user will have a folder in a shared bucket under the folder structure: *bucket/home/%username%*.

What steps should a Solutions Architect take to ensure that each user can access their own home folder and no one else's? (Select TWO.)

1. Create a bucket policy that applies access permissions based on username
2. Create an IAM policy that applies folder-level permissions
3. Create an IAM policy that applies object-level S3 ACLs
4. Attach an S3 ACL sub-resource that grants access based on the %username% variable
5. Create an IAM group and attach the IAM policy, add IAM users to the group

QUESTION 46

An event in CloudTrail is the record of an activity in an AWS account. What are the two types of events that can be logged in CloudTrail? (Select TWO.)

1. Platform Events which are also known as hardware level operations
2. Data Events which are also known as data plane operations
3. System Events which are also known as instance level operations
4. Control Events which are also known as data plane operations
5. Management Events which are also known as control plane operations

QUESTION 47

A Solutions Architect is writing some code that uses an AWS Lambda function and would like to enable the function to connect

to an Amazon ElastiCache cluster within an Amazon VPC in the same AWS account. What VPC-specific information must be included in the function to enable this configuration? (Select TWO.)

1. VPC Subnet IDs
2. VPC Logical IDs
3. VPC Peering IDs
4. VPC Security Group IDs
5. VPC Route Table IDs

QUESTION 48

A Solutions Architect created a new subnet in an Amazon VPC and launched an Amazon EC2 instance into it. The Solutions Architect needs to directly access the EC2 instance from the Internet and cannot connect. Which steps should be undertaken to troubleshoot the issue? (Select TWO.)

1. Check that the instance has a public IP address
2. Check that there is a NAT Gateway configured for the subnet
3. Check that Security Group has a rule for outbound traffic
4. Check that the route table associated with the subnet has an entry for an Internet Gateway
5. Check that you can ping the instance from another subnet

QUESTION 49

A Solutions Architect just completed the implementation of a 2-tier web application for a client. The application uses Amazon EC2 instances, Amazon ELB and Auto Scaling across two subnets. After deployment the Solutions Architect noticed that only one subnet has EC2 instances running in it. What might be the cause of this situation?

1. The ELB is configured as an internal-only load balancer
2. The Auto Scaling Group has not been configured with multiple subnets
3. Cross-zone load balancing is not enabled on the ELB
4. The AMI is missing from the ASG's launch configuration

QUESTION 50

A Solutions Architect is designing the messaging and streaming layers of a serverless application. The messaging layer will manage communications between components and the streaming layer will manage real-time analysis and processing of streaming data.

The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the messaging and streaming layers? (Select TWO.)

1. Use Amazon Kinesis for collecting, processing and analyzing real-time streaming data
2. Use Amazon SWF for providing a fully managed messaging service
3. Use Amazon SNS for providing a fully managed messaging service
4. Use Amazon EMR for collecting, processing and analyzing real-time streaming data
5. Use AWS CloudTrail for collecting, processing and analyzing real-time streaming data

QUESTION 51

An existing Auto Scaling group is running with eight Amazon EC2 instances. A Solutions Architect has attached an Elastic Load Balancer (ELB) to the Auto Scaling group by connecting a Target Group. The ELB is in the same region and already has ten EC2 instances running in the Target Group.

When attempting to attach the ELB the request immediately fails, what is the MOST likely cause?

1. Adding the 10 EC2 instances to the ASG would exceed the maximum capacity configured
2. One or more of the instances are unhealthy
3. ASGs cannot be edited once defined, you would need to recreate it
4. You cannot attach running EC2 instances to an ASG

QUESTION 52

The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited

security violations and network abuse. According to the policy, what is AWS's position on penetration testing?

1. AWS do not allow any form of penetration testing
2. AWS allow penetration testing by customers on their own VPC resources
3. AWS allow penetration for some resources without prior authorization
4. AWS allow penetration testing for all resources

QUESTION 53

An application regularly uploads files from an Amazon EC2 instance to an Amazon S3 bucket. The files can be a couple of gigabytes in size and sometimes the uploads are slower than desired. What method can be used to increase throughput and reduce upload times?

1. Turn off versioning on the destination bucket
2. Randomize the object names when uploading
3. Use Amazon S3 multipart upload
4. Upload the files using the S3 Copy SDK or REST API

QUESTION 54

A three-tier web application that is deployed in an Amazon VPC has been experiencing heavy load on the database layer. The database layer uses an Amazon RDS MySQL instance in a multi-AZ configuration. Customers have been complaining about poor response times. During troubleshooting it has been noted that the database layer is experiencing high read contention during peak hours of the day.

What are two possible options that could be used to offload some of the read traffic from the database to resolve the performance issues? (Select TWO.)

1. Add RDS read replicas in each AZ
2. Use an ELB to distribute load between RDS instances
3. Migrate to DynamoDB
4. Use a larger RDS instance size
5. Deploy ElastiCache in each AZ

QUESTION 55

A Solutions Architect is creating a multi-tier application that includes loosely-coupled, distributed application components and needs to determine a method of sending notifications instantaneously. Using Amazon SNS which transport protocols are supported? (Select TWO.)

1. Amazon SWF
2. FTP
3. HTTPS
4. AWS Lambda
5. Email-JSON

QUESTION 56

A manager is concerned that the default service limits may soon be reached for several AWS services. Which AWS tool can a Solutions Architect use to display current usage and limits?

1. AWS Systems Manager
2. AWS Trusted Advisor
3. AWS Dashboard
4. Amazon CloudWatch

QUESTION 57

A company has multiple AWS accounts for several environments (Prod, Dev, Test etc.). A Solutions Architect would like to copy an Amazon EBS snapshot from DEV to PROD. The snapshot is from an EBS volume that was encrypted with a custom key.

What steps must be performed to share the encrypted EBS snapshot with the Prod account? (Select TWO.)

1. Share the custom key used to encrypt the volume

2. Make a copy of the EBS volume and unencrypt the data in the process
3. Create a snapshot of the unencrypted volume and share it with the Prod account
4. Modify the permissions on the encrypted snapshot to share it with the Prod account
5. Use CloudHSM to distribute the encryption keys use to encrypt the volume

QUESTION 58

An application you manage runs a number of components using a micro-services architecture. Several ECS container instances in your ECS cluster are displaying as disconnected. The ECS instances were created from the Amazon ECS-Optimized AMI. What steps might you take to troubleshoot the issue? (Select TWO.)

1. Verify that the instances have the correct IAM group applied
2. Verify that the container instances have the container agent installed
3. Verify that the IAM instance profile has the necessary permissions
4. Verify that the container agent is running on the container instances
5. Verify that the container instances are using the Fargate launch type

QUESTION 59

The application development team in a company have created a new application written in .NET. A Solutions Architect is looking for a way to easily deploy the application whilst maintaining full control of the underlying resources.

Which PaaS service provided by AWS would BEST suit this requirement?

1. CloudFront
2. Elastic Beanstalk
3. EC2 Placement Groups
4. CloudFormation

QUESTION 60

A Solutions Architect is building a small web application running on Amazon EC2 that will be serving static content. The user base is spread out globally and speed is important. Which AWS service can deliver the best user experience cost-effectively and reduce the load on the web server?

1. Amazon RedShift
2. Amazon S3
3. Amazon CloudFront
4. Amazon EBS volume

QUESTION 61

Amazon CloudWatch is being used to monitor the performance of AWS Lambda. Which metrics does Lambda track? (Select TWO.)

1. Total number of requests
2. Latency per request
3. Number of users
4. Total number of connections
5. Total number of transactions

QUESTION 62

An Amazon EC2 instance running a video on demand web application has been experiencing high CPU utilization. A Solutions Architect needs to take steps to reduce the impact on the EC2 instance and improve performance for consumers. Which of the steps below would help?

1. Use ElastiCache as the web front-end and forward connections to EC2 for cache misses
2. Create a CloudFront distribution and configure a custom origin pointing at the EC2 instance
3. Create an ELB and place it in front of the EC2 instance
4. Create a CloudFront RTMP distribution and point it at the EC2 instance

QUESTION 63

A Solutions Architect needs to create a file system that can be concurrently accessed by multiple Amazon EC2 instances across multiple availability zones. The file system needs to support high throughput and the ability to burst. As the data that will be stored on the file system will be sensitive, it must be encrypted at rest and in transit.

Which storage solution should the Solutions Architect use for the shared file system?

1. Add EBS volumes to each EC2 instance and configure data replication
2. Use the Elastic Block Store (EBS) and mount the file system at the block level
3. Use the Elastic File System (EFS) and mount the file system using NFS
4. Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

QUESTION 64

A new department will begin using AWS services an AWS account and a Solutions Architect needs to create an authentication and authorization strategy. Select the correct statements regarding IAM groups? (Select TWO.)

1. IAM groups can be used to assign permissions to users
2. IAM groups can be nested up to 4 levels
3. IAM groups can be used to group EC2 instances
4. IAM groups can temporarily assume a role to take on permissions for a specific task
5. An IAM group is not an identity and cannot be identified as a principal in an IAM policy

QUESTION 65

The development team in a media organization is moving their SDLC processes into the AWS Cloud. Which AWS service can a Solutions Architect recommend that is primarily used for software version control?

1. CloudHSM
2. CodeStar
3. CodeCommit
4. Step Functions

SET 5: PRACTICE QUESTIONS AND ANSWERS

QUESTION 1

A Solutions Architect has deployed an API using Amazon API Gateway and created usage plans and API keys for several customers. Requests from one particular customer have been excessive and the solutions architect needs to limit the rate of requests. Other customers should not be affected. How should the solutions architect proceed?

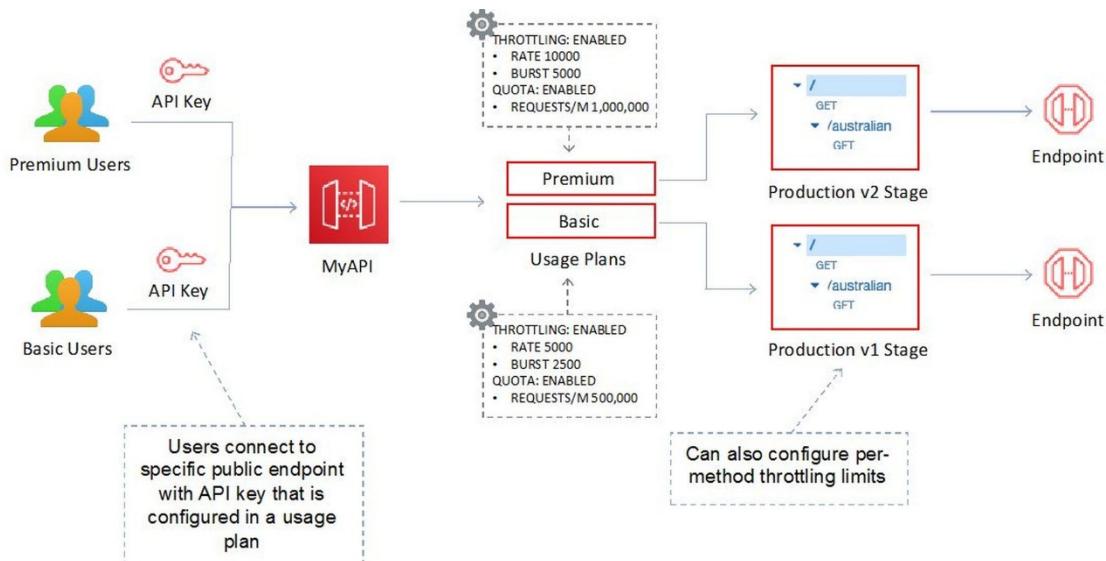
1. Configure a server-side throttling limit
2. Configure the per-method throttling limits
3. Configure per-client throttling limits
4. Configure the account-level throttling limits

Answer: 3

Explanation:

Per-client throttling limits are applied to clients that use API keys associated with your usage policy as client identifier. This can be applied to the single customer that is issuing excessive API requests. This is the best option to ensure that only one customer is affected.

In the diagram below, per-client throttling limits are set in a usage plan:



CORRECT: "Configure per-client throttling limits" is the correct answer.

INCORRECT: "Configure a server-side throttling limit" is incorrect. Server-side throttling limits are applied across all clients. These limit settings exist to prevent your API—and your account—from being overwhelmed by too many requests. In this case, the solutions architect need to apply the throttling to a single client.

INCORRECT: "Configure the per-method throttling limits" is incorrect. Per-method throttling limits apply to all customers using the same method. This will affect all customers who are using the API.

INCORRECT: "Configure the account-level throttling limits" is incorrect. Account-level throttling limits define the maximum steady-state request rate and burst limits for the account. This does not apply to individual customers.

References:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/>

QUESTION 2

A Solutions Architect is deploying a high performance computing (HPC) application on Amazon EC2 instances. The application requires extremely low inter-instance latency. How should the instances be deployed for BEST performance?

1. Use an instance with enhanced networking and deploy the instances in a partition placement group
2. Use an Elastic Fabric Adapter (EFA) and deploy instances in a cluster placement group
3. Add multiple Elastic Network Adapters (ENAs) to each instance and create a NIC team
4. Use an EBS-optimized instance with 10 Gigabit networking and deploy to a single subnet

Answer: 2

Explanation:

It is recommended to use either enhanced networking or an Elastic Fabric Adapter (EFA) for the nodes of an HPC application. This will assist with decreasing latency. Additionally, a cluster placement group packs instances close together inside an Availability Zone.

Using a cluster placement group enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

The table below helps you to understand the key differences between the different placement group options:

	Clustered	Spread	Partition
What	Instances are placed into a low-latency group within a single AZ	Instances are spread across underlying hardware	Instances are grouped into logical segments called partitions which use distinct hardware
When	Need low network latency and/or high network throughput	Reduce the risk of simultaneous instance failure if underlying hardware fails	Need control and visibility into instance placement
Pros	Get the most out of enhanced networking Instances	Can span multiple AZs	Reduces likelihood of correlated failures for large workloads.
Cons	Finite capacity: recommend launching all you might need up front	Maximum of 7 instances running per group, per AZ	Partition placement groups are not supported for Dedicated Hosts

CORRECT: "Use an Elastic Fabric Adapter (EFA) and deploy instances in a cluster placement group" is the correct answer.

INCORRECT: "Use an instance with enhanced networking and deploy the instances in a partition placement group" is incorrect. A partition placement group protects instances from correlated hardware failures, it does not offer the best inter-instance network performance.

INCORRECT: "Add multiple Elastic Network Adapters (ENAs) to each instance and create a NIC team" is incorrect. You cannot use NIC teaming methods on AWS to increase the bandwidth to your application. This will also not reduce latency.

INCORRECT: "Use an EBS-optimized instance with 10 Gigabit networking and deploy to a single subnet" is incorrect. EBS optimization is related to storage, not to network performance. A 10 Gigabit adapter offers great bandwidth but for lowest latency enhanced networking with a cluster placement group should be used.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 3

A company has deployed an API using Amazon API Gateway. There are many repeat requests and a solutions architect has been asked to implement measures to reduce request latency and the number of calls to the Amazon EC2 endpoint.

How can this be most easily achieved?

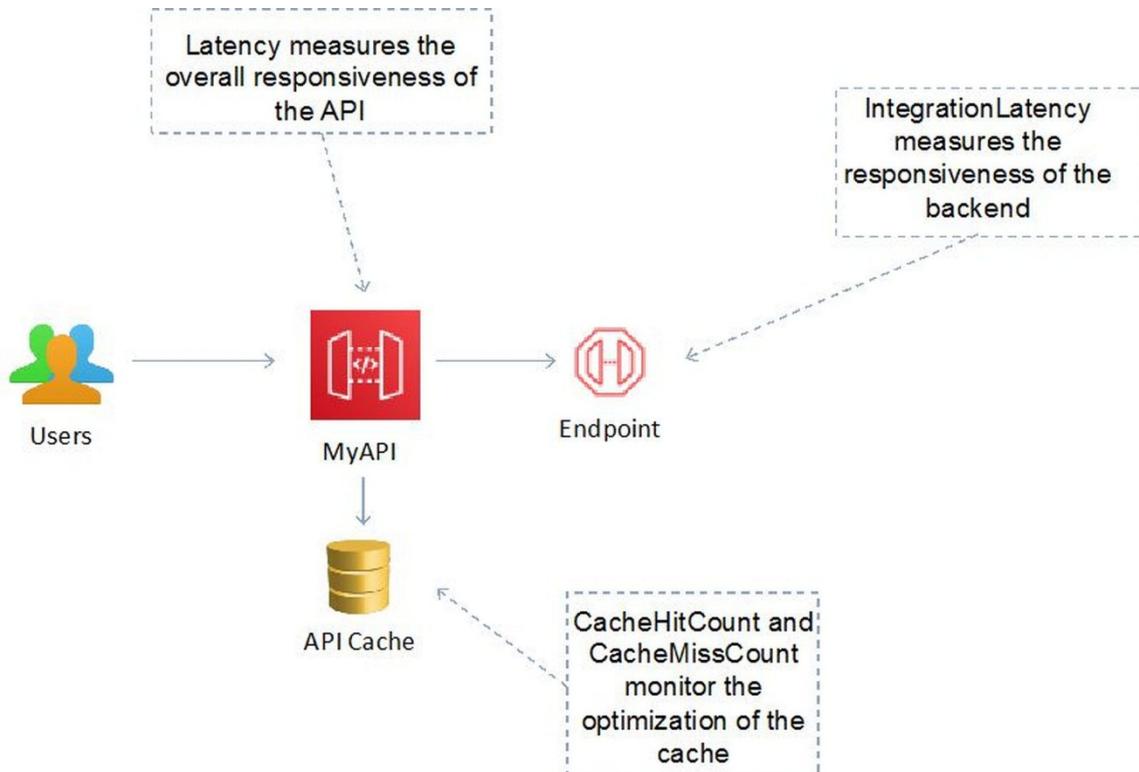
1. Create a cache for a stage and configure a TTL
2. Create a cache for a method and configure a TTL
3. Configure an edge-optimized endpoint with CloudFront
4. Configure a private endpoint place ElastiCache in front

Answer: 1

Explanation:

You can enable API caching in Amazon API Gateway to cache your endpoint's responses. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API.

When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds. API Gateway then responds to the request by looking up the endpoint response from the cache instead of making a request to your endpoint. The default TTL value for API caching is 300 seconds. The maximum TTL value is 3600 seconds. TTL=0 means caching is disabled.



CORRECT: "Create a cache for a stage and configure a TTL" is the correct answer.

INCORRECT: "Create a cache for a method and configure a TTL" is incorrect. An API cache is not enabled for a method, it is enabled for a stage.

INCORRECT: "Configure an edge-optimized endpoint with CloudFront" is incorrect. This is the default endpoint type with API Gateway so there's no reason to believe the solution architect needs to configure this. Users are routed to the nearest

CloudFront point of presence (POP). However, caching still takes place within API gateway using a stage cache.

INCORRECT: "Configure a private endpoint place ElastiCache in front" is incorrect. You cannot use Amazon ElastiCache to cache API requests.

References:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/>

QUESTION 4

A Solutions Architect is designing a migration strategy for a company moving to the AWS Cloud. The company uses a shared Microsoft filesystem that uses Distributed File System Namespaces (DFSN). What will be the MOST suitable migration strategy for the filesystem?

1. Use the AWS Server Migration Service to migrate to an Amazon S3 bucket
2. Use the AWS Server Migration Service to migrate to Amazon FSx for Lustre
3. Use AWS DataSync to migrate to an Amazon EFS filesystem
4. Use AWS DataSync to migrate to Amazon FSx for Windows File Server

Answer: 4

Explanation:

The destination filesystem should be Amazon FSx for Windows File Server. This supports DFSN and is the most suitable storage solution for Microsoft filesystems. AWS DataSync supports migrating to the Amazon FSx and automates the process.

CORRECT: "Use AWS DataSync to migrate to Amazon FSx for Windows File Server" is the correct answer.

INCORRECT: "Use the AWS Server Migration Service to migrate to Amazon FSx for Lustre" is incorrect. The server migration service is used to migrate virtual machines and FSx for Lustre does not support Windows filesystems.

INCORRECT: "Use AWS DataSync to migrate to an Amazon EFS filesystem" is incorrect. You can migrate data to EFS using DataSync but it is the wrong destination for a Microsoft filesystem (Linux only).

INCORRECT: "Use the AWS Server Migration Service to migrate to an Amazon S3 bucket" is incorrect. The server migration service is used to migrate virtual machines and Amazon S3 is an object-based storage system and unsuitable for hosting a Microsoft filesystem.

References:

<https://aws.amazon.com/blogs/storage/migrate-to-amazon-fsx-for-windows-file-server-using-aws-datasync/>

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-fsx.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

QUESTION 5

An Amazon ElastiCache for Redis cluster runs across multiple Availability Zones. A solutions architect is concerned about the security of sensitive data as it is replicated between nodes. How can the solutions architect protect the sensitive data?

1. Issue a Redis AUTH command
2. Enable in-transit encryption
3. Enable at-rest encryption
4. Set up MFA and API logging

Answer: 2

Explanation:

Amazon ElastiCache in-transit encryption is an optional feature that allows you to increase the security of your data at its most vulnerable points—when it is in transit from one location to another. Because there is some processing needed to encrypt and decrypt the data at the endpoints, enabling in-transit encryption can have some performance impact. You should benchmark

your data with and without in-transit encryption to determine the performance impact for your use cases.

ElastiCache in-transit encryption implements the following features:

- **Encrypted connections**—both the server and client connections are Secure Socket Layer (SSL) encrypted.
- **Encrypted replication**—data moving between a primary node and replica nodes is encrypted.
- **Server authentication**—clients can authenticate that they are connecting to the right server.
- **Client authentication**—using the Redis AUTH feature, the server can authenticate the clients.

CORRECT: "Enable in-transit encryption" is the correct answer.

INCORRECT: "Issue a Redis AUTH command" is incorrect. This is used when using a password to access the database.

INCORRECT: "Enable at-rest encryption" is incorrect. ElastiCache for Redis at-rest encryption is an optional feature to increase data security by encrypting on-disk data. This does not encrypt the data in-transit when it is being replicated between nodes.

INCORRECT: "Set up MFA and API logging" is incorrect. Neither multi-factor authentication or API logging is going to assist with encrypting data.

References:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/at-rest-encryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticsearch/>

QUESTION 6

A company runs an application on-premises that must consume a REST API running on Amazon API Gateway. The company has an AWS Direct Connect connection to their Amazon VPC. The solutions architect wants all API calls to use private addressing only and avoid the internet. How can this be achieved?

1. Use a transit virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway
2. Use a private virtual interface and create a VPC Endpoint for Amazon API Gateway
3. Use a hosted virtual interface and create a VPC Endpoint for Amazon API Gateway
4. Use a public virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway

Answer: 2

Explanation:

The requirements are to avoid the internet and use private IP addresses only. The best solution is to use a private virtual interface across the Direct Connect connection to connect to the VPC using private IP addresses. A VPC endpoint for Amazon API Gateway can be created and this will provide access to API Gateway using private IP addresses and avoids the internet completely.

CORRECT: "Use a private virtual interface and create a VPC Endpoint for Amazon API Gateway" is the correct answer.

INCORRECT: "Use a hosted virtual interface and create a VPC Endpoint for Amazon API Gateway" is incorrect. A hosted virtual interface is used to allow another account to access your Direct Connect link.

INCORRECT: "Use a transit virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway" is incorrect. A transit virtual interface is used to access Amazon VPC Transit Gateways which are not included in the solution.

INCORRECT: "Use a public virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway" is incorrect. This will use the public internet so it is not allowed in this scenario.

References:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 7

A company has an eCommerce application that runs from multiple AWS Regions. Each region has a separate database running on Amazon EC2 instances. The company plans to consolidate the data to a columnar database and run analytics queries. Which approach should the company take?

1. Run an AWS Batch job to copy and process the data into a columnar Amazon RDS database. Use Amazon Athena to analyze the data
2. Use the COPY command to load data into an Amazon RedShift data warehouse and run the analytics queries there
3. Launch Amazon Kinesis Data Streams producers to load data into a Kinesis Data stream. Use Kinesis Data Analytics to analyze the data
4. Create an AWS Lambda function that copies the data onto Amazon S3. Use Amazon S3 Select to query the data

Answer: 2

Explanation:

Amazon Redshift is an enterprise-level, petabyte scale, fully managed data warehousing service. It uses columnar storage to improve the performance of complex queries.

You can use the COPY command to load data in parallel from one or more remote hosts, such Amazon EC2 instances or other computers. COPY connects to the remote hosts using SSH and executes commands on the remote hosts to generate text output.

CORRECT: "Use the COPY command to load data into an Amazon RedShift data warehouse and run the analytics queries there" is the correct answer.

INCORRECT: "Run an AWS Batch job to copy and process the data into a columnar Amazon RDS database. Use Amazon Athena to analyze the data" is incorrect. AWS Batch is used for running batch computing jobs across a fleet of EC2 instances. You cannot create a "columnar Amazon RDS database" as RDS is optimized for transactional workloads. Athena is used to analyze data on S3.

INCORRECT: "Launch Amazon Kinesis Data Streams producers to load data into a Kinesis Data stream. Use Kinesis Data Analytics to analyze the data" is incorrect. Kinesis is a real-time streaming data service. It is not a columnar database so is unsuitable for this use case.

INCORRECT: "Create an AWS Lambda function that copies the data onto Amazon S3. Use Amazon S3 Select to query the data" is incorrect. S3 is not a columnar database and S3 select does not run analytics queries, it simply selects data from an object to retrieve.

References:

<https://docs.aws.amazon.com/redshift/latest/dg/loading-data-from-remote-hosts.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>

QUESTION 8

There has been an increase in traffic to an application that writes data to an Amazon DynamoDB database. Thousands of random tables reads occur per second and low-latency is required. What can a Solutions Architect do to improve performance for the reads without negatively impacting the rest of the application?

1. Increase the number of Amazon DynamoDB write capacity units
2. Add an Amazon SQS queue to decouple the requests
3. Use Amazon DynamoDB Accelerator to cache the reads
4. Use an Amazon Kinesis Data Stream to decouple requests

Answer: 3

Explanation:

DAX is a DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding

applications. DAX addresses three core scenarios:

1. As an in-memory cache, DAX reduces the response times of eventually consistent read workloads by an order of magnitude from single-digit milliseconds to microseconds.
2. DAX reduces operational and application complexity by providing a managed service that is API-compatible with DynamoDB. Therefore, it requires only minimal functional changes to use with an existing application.
3. For read-heavy or bursty workloads, DAX provides increased throughput and potential operational cost savings by reducing the need to overprovision read capacity units. This is especially beneficial for applications that require repeated reads for individual keys.

DynamoDB accelerator is the best solution for caching the reads and delivering them at extremely low latency.

CORRECT: "Use Amazon DynamoDB Accelerator to cache the reads" is the correct answer.

INCORRECT: "Increase the number of Amazon DynamoDB write capacity units" is incorrect. This will not improve read performance as write capacity units affect write performance.

INCORRECT: "Add an Amazon SQS queue to decouple the requests" is incorrect. You cannot decouple a database from the frontend with a queue in order to decrease read latency.

INCORRECT: "Use an Amazon Kinesis Data Stream to decouple requests" is incorrect. You cannot increase read performance for a database by implementing a real-time streaming service.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

QUESTION 9

A Solutions Architect must enable an application to download software updates from the internet. The application runs on a series of EC2 instances in an Auto Scaling group running in a private subnet. The solution must involve minimal ongoing systems management effort. How should the Solutions Architect proceed?

1. Implement a NAT gateway
2. Launch a NAT instance
3. Create a Virtual Private Gateway
4. Attach Elastic IP addresses

Answer: 1

Explanation:

Both a NAT gateway or a NAT instance can be used for this use case. Both services enable internet access for instances in private subnets. However, the NAT instance runs on an EC2 instance you must launch, configure and manage and therefore involves more ongoing systems management effort.

CORRECT: "Implement a NAT gateway" is the correct answer.

INCORRECT: "Launch a NAT instance" is incorrect as this service involves more ongoing systems management effort.

INCORRECT: "Create a Virtual Private Gateway" is incorrect. A VPG is used as part of a VPN connection (AWS side of the connection). It is not used to enable internet access.

INCORRECT: "Attach Elastic IP addresses" is incorrect. You cannot use Elastic IP addresses with instances in private subnets.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 10

A Solutions Architect manages multiple Amazon RDS MySQL databases. To improve security, the Solutions Architect wants to

enable secure user access with short-lived credentials. How can these requirements be met?

1. Configure the MySQL databases to use the AWS Security Token Service (STS)
2. Configure the application to use the AUTH command to send a unique password
3. Create the MySQL user accounts to use the AWSAuthenticationPlugin with IAM
4. Configure the MySQL databases to use AWS KMS data encryption keys

Answer: 3

Explanation:

With MySQL, authentication is handled by AWSAuthenticationPlugin—an AWS-provided plugin that works seamlessly with IAM to authenticate your IAM users. Connect to the DB instance and issue the CREATE USER statement, as shown in the following example.

CREATE USER jane_doe IDENTIFIED WITH AWSAuthenticationPlugin AS 'RDS';

The IDENTIFIED WITH clause allows MySQL to use the AWSAuthenticationPlugin to authenticate the database account (jane_doe). The AS 'RDS' clause refers to the authentication method, and the specified database account should have the same name as the IAM user or role. In this example, both the database account and the IAM user or role are named jane_doe.

CORRECT: "Create the MySQL user accounts to use the AWSAuthenticationPlugin with IAM" is the correct answer.

INCORRECT: "Configure the MySQL databases to use the AWS Security Token Service (STS)" is incorrect. You cannot configure MySQL to directly use the AWS STS.

INCORRECT: "Configure the application to use the AUTH command to send a unique password" is incorrect. This is used with Redis databases, not with RDS databases.

INCORRECT: "Configure the MySQL databases to use AWS KMS data encryption keys" is incorrect. Data encryption keys are used for data encryption not management of connection strings.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.DBAccounts.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 11

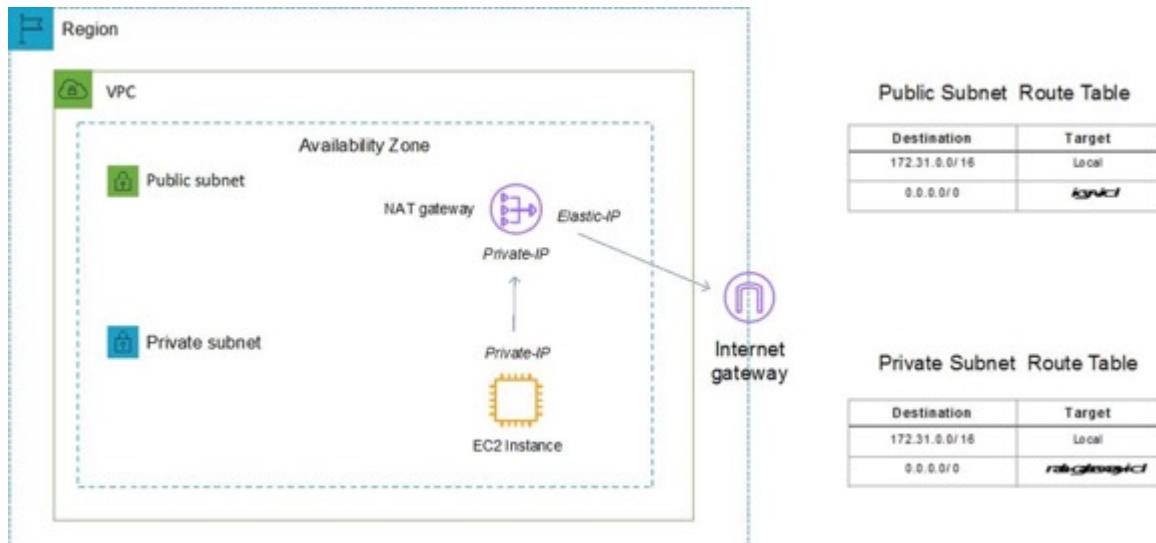
An application is running in a private subnet of an Amazon VPC and must have outbound internet access for downloading updates. The Solutions Architect does not want the application exposed to inbound connection attempts. Which steps should be taken?

1. Create a NAT gateway but do not attach an internet gateway to the VPC
2. Attach an internet gateway to the private subnet and create a NAT gateway
3. Attach an internet gateway to the VPC but do not create a NAT gateway
4. Create a NAT gateway and attach an internet gateway to the VPC

Answer: 4

Explanation:

To enable outbound connectivity for instances in private subnets a NAT gateway can be created. The NAT gateway is created in a public subnet and a route must be created in the private subnet pointing to the NAT gateway for internet-bound traffic. An internet gateway must be attached to the VPC to facilitate outbound connections.



You cannot directly connect to an instance in a private subnet from the internet. You would need to use a bastion/jump host. Therefore, the application will not be exposed to inbound connection attempts.

CORRECT: "Create a NAT gateway and attach an internet gateway to the VPC" is the correct answer.

INCORRECT: "Create a NAT gateway but do not create attach an internet gateway to the VPC" is incorrect. An internet gateway must be attached to the VPC for any outbound connections to work.

INCORRECT: "Attach an internet gateway to the private subnet and create a NAT gateway" is incorrect. You do not attach internet gateways to subnets, you attach them to VPCs.

INCORRECT: "Attach an internet gateway to the VPC but do not create a NAT gateway" is incorrect. Without a NAT gateway the instances in the private subnet will not be able to download updates from the internet.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 12

An application has been migrated from on-premises to an Amazon EC2 instance. The migration has failed to an unknown dependency that the application must communicate with an on-premises server using private IP addresses.

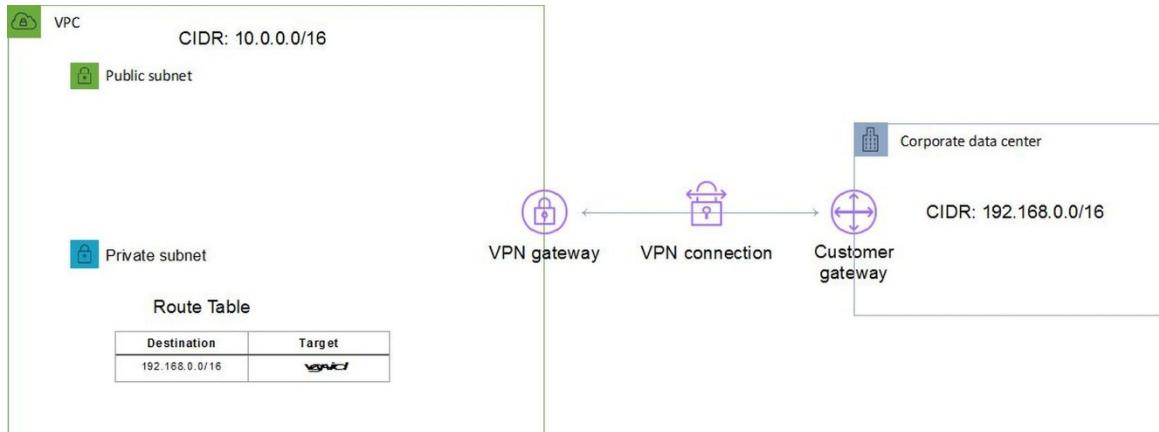
Which action should a solutions architect take to quickly provision the necessary connectivity?

1. Setup an AWS Direct Connect connection
2. Configure a Virtual Private Gateway
3. Create an Amazon CloudFront distribution
4. Create an AWS Transit Gateway

Answer: 2

Explanation:

A virtual private gateway is a logical, fully redundant distributed edge routing function that sits at the edge of your VPC. You must create a VPG in your VPC before you can establish an AWS Managed site-to-site VPN connection. The other end of the connection is the customer gateway which must be established on the customer side of the connection.



CORRECT: "Configure a Virtual Private Gateway" is the correct answer.

INCORRECT: "Setup an AWS Direct Connect connection" is incorrect as this would take too long to provision.

INCORRECT: "Create an Amazon CloudFront distribution" is incorrect. This is not a solution for enabling connectivity using private addresses to an on-premises site. CloudFront is a content delivery network (CDN).

INCORRECT: "Create an AWS Transit Gateway" is incorrect. AWS Transit Gateway connects VPCs and on-premises networks through a central hub which is not a requirement of this solution.

References:

https://docs.aws.amazon.com/vpn/latest/s2vpn/VPC_VPN.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 13

A company runs an API on a Linux server in their on-premises data center. The company are planning to migrate the API to the AWS cloud. The company require a highly available, scalable and cost-effective solution. What should a Solutions Architect recommend?

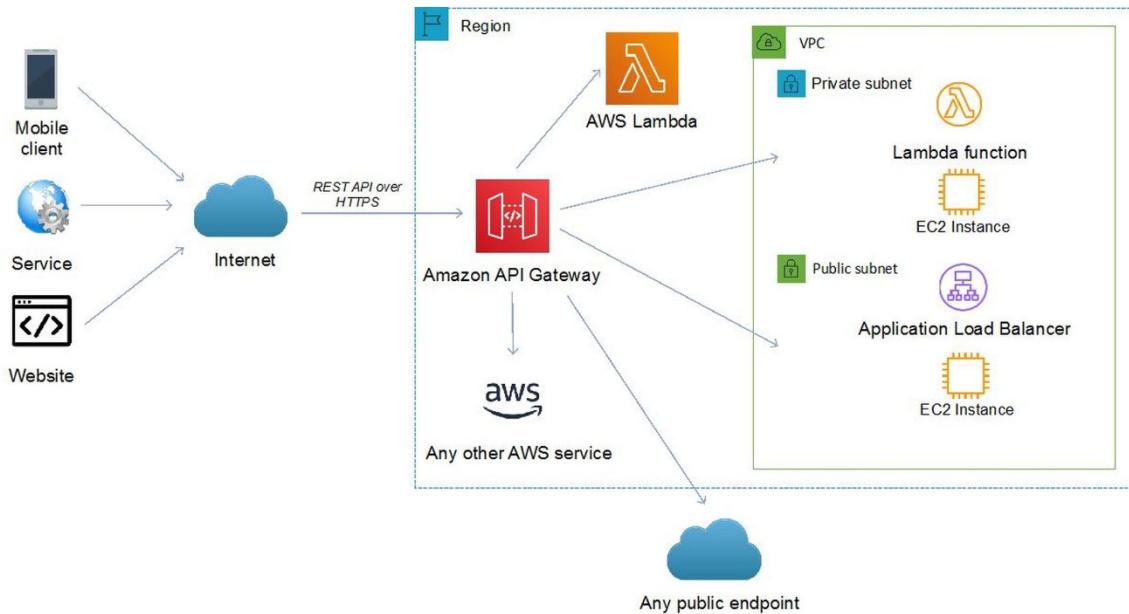
1. Migrate the API to Amazon API Gateway and migrate the backend to Amazon EC2
2. Migrate the API server to Amazon EC2 instances in an Auto Scaling group and attach an Application Load Balancer
3. Migrate the API to Amazon API Gateway and use AWS Lambda as the backend
4. Migrate the API to Amazon CloudFront and use AWS Lambda as the origin

Answer: 3

Explanation:

The best option is to use a fully serverless solution. This will provide high availability, scalability and be cost-effective. The components for this would be Amazon API Gateway for hosting the API and AWS Lambda for running the backend.

As you can see in the image below, API Gateway can be the frontend for multiple backend services:



CORRECT: "Migrate the API to Amazon API Gateway and use AWS Lambda as the backend" is the correct answer.

INCORRECT: "Migrate the API to Amazon API Gateway and migrate the backend to Amazon EC2" is incorrect. This is a less available and cost-effective solution for the backend compared to AWS Lambda.

INCORRECT: "Migrate the API server to Amazon EC2 instances in an Auto Scaling group and attach an Application Load Balancer" is incorrect. Firstly, it may be difficult to load balance to an API. Additionally, this is a less cost-effective solution.

INCORRECT: "Migrate the API to Amazon CloudFront and use AWS Lambda as the origin" is incorrect. You cannot migrate an API to CloudFront. You can use CloudFront in front of API Gateway but that is not what this answer specifies.

References:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-with-lambda-integration.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

QUESTION 14

An application that is being installed on an Amazon EC2 instance requires a persistent block storage volume. The data must be encrypted at rest and regular volume-level backups must be automated.

Which solution options should be used?

1. Use an encrypted Amazon EBS volume and use Data Lifecycle Manager to automate snapshots
2. Use an encrypted Amazon EFS filesystem and use an Amazon CloudWatch Events rule to start a backup copy of data using AWS Lambda
3. Use server-side encryption on an Amazon S3 bucket and use Cross-Region-Replication to backup on a schedule
4. Use an encrypted Amazon EC2 instance store and copy the data to another EC2 instance using a cron job and a batch script

Answer: 1

Explanation:

For block storage the Solutions Architect should use either Amazon EBS or EC2 instance store. However, the instance store is non-persistent so EBS must be used. With EBS you can encrypt your volume and automate volume-level backups using snapshots that are run by Data Lifecycle Manager.

CORRECT: "Use an encrypted Amazon EBS volume and use Data Lifecycle Manager to automate snapshots" is the correct answer.

INCORRECT: "Use an encrypted Amazon EFS filesystem and use an Amazon CloudWatch Events rule to start a backup copy of data using AWS Lambda" is incorrect. EFS is not block storage, it is a file-level storage service.

INCORRECT: "Use server-side encryption on an Amazon S3 bucket and use Cross-Region-Replication to backup on a schedule" is incorrect. Amazon S3 is an object-based storage system not a block-based storage system.

INCORRECT: "Use an encrypted Amazon EC2 instance store and copy the data to another EC2 instance using a cron job and a batch script" is incorrect as the EC2 instance store is a non-persistent volume.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 15

A company has several AWS accounts each with multiple Amazon VPCs. The company must establish routing between all private subnets. The architecture should be simple and allow transitive routing to occur.

How should the network connectivity be configured?

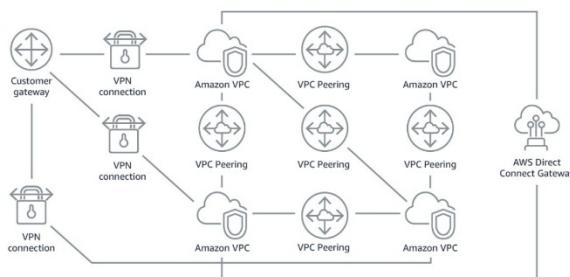
1. Create a transitive VPC peering connection between each Amazon VPC and configure route tables
2. Create an AWS Transit Gateway and share it with each account using AWS Resource Access Manager
3. Create an AWS Managed VPN between each Amazon VPC and configure route tables
4. Create a hub-and-spoke topology with AWS App Mesh and use AWS Resource Access Manager to share route tables

Answer: 2

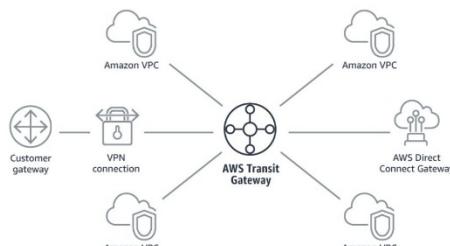
Explanation:

You can build a hub-and-spoke topology with AWS Transit Gateway that supports transitive routing. This simplifies the network topology and adds additional features over VPC peering. AWS Resource Access Manager can be used to share the connection with the other AWS accounts.

Without AWS Transit Gateway



With AWS Transit Gateway



CORRECT: "Create an AWS Transit Gateway and share it with each account using AWS Resource Access Manager" is the correct answer.

INCORRECT: "Create a transitive VPC peering connection between each Amazon VPC and configure route tables" is incorrect. You cannot create transitive connections with VPC peering.

INCORRECT: "Create an AWS Managed VPN between each Amazon VPC and configure route tables" is incorrect. This is a much more complex solution compared to AWS Transit Gateway so is not the best option.

INCORRECT: "Create a hub-and-spoke topology with AWS App Mesh and use AWS Resource Access Manager to share route tables" is incorrect. AWS App Mesh is used for application-level networking for microservices applications.

References:

<https://aws.amazon.com/blogs/aws/new-use-an-aws-transit-gateway-to-simplify-your-network-architecture/>

Save time with our exam-specific cheat sheets:

QUESTION 16

An organization is planning their disaster recovery solution. They plan to run a scaled down version of a fully functional environment. In a DR situation the recovery time must be minimized.

Which DR strategy should a Solutions Architect recommend?

1. Backup and restore
2. Pilot light
3. Warm standby
4. Multi-site

Answer: 3

Explanation:

The term warm standby is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud. A warm standby solution extends the pilot light elements and preparation.

It further decreases the recovery time because some services are always running. By identifying your business-critical systems, you can fully duplicate these systems on AWS and have them always on.

CORRECT: "Warm standby" is the correct answer.

INCORRECT: "Backup and restore" is incorrect. This is the lowest cost DR approach that simply entails creating online backups of all data and applications.

INCORRECT: "Pilot light"" is incorrect. With a pilot light strategy a core minimum of services are running and the remainder are only brought online during a disaster recovery situation.

INCORRECT: "Multi-site" is incorrect. A multi-site solution runs on AWS as well as on your existing on-site infrastructure in an active- active configuration.

References:

QUESTION 17

An application analyzes images of people that are uploaded to an Amazon S3 bucket. The application determines demographic data which is then saved to a .CSV file in another S3 bucket. The data must be encrypted at rest and then queried using SQL. The solution should be fully serverless.

Which actions should a Solutions Architect take to encrypt and query the data?

1. Use Amazon S3 server-side encryption and use Amazon RedShift Spectrum to query the data
2. Use AWS KMS encryption keys for the S3 bucket and use Amazon Athena to query the data
3. Use AWS KMS encryption keys for the S3 bucket and use Amazon Kinesis Data Analytics to query the data
4. Use Amazon S3 server-side encryption and Amazon QuickSight to query the data

Answer: 2

Explanation:

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. Amazon Athena supports encrypted data for both the source data and query results, for example, using Amazon S3 with AWS KMS.

CORRECT: "Use AWS KMS encryption keys for the S3 bucket and use Amazon Athena to query the data" is the correct answer.

INCORRECT: "Use Amazon S3 server-side encryption and use Amazon RedShift Spectrum to query the data" is incorrect. RedShift Spectrum is not serverless as it requires a RedShift cluster which is based on EC2 instances.

INCORRECT: "Use AWS KMS encryption keys for the S3 bucket and use Amazon Kinesis Data Analytics to query the data" is incorrect. Kinesis Data Analytics is used for analyzing real-time streaming data in Kinesis streams.

INCORRECT: "Use Amazon S3 server-side encryption and Amazon QuickSight to query the data" is incorrect. Amazon QuickSight is an interactive dashboard, it is not a service for running queries on data.

References:

<https://d1.awsstatic.com/whitepapers/architecture/wellarchitected-Machine-Learning-Lens.pdf>

<https://aws.amazon.com/athena/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-athena/>

QUESTION 18

A large quantity of data is stored on a NAS device on-premises and accessed using the SMB protocol. The company require a managed service for hosting the filesystem and a tool to automate the migration.

Which actions should a Solutions Architect take?

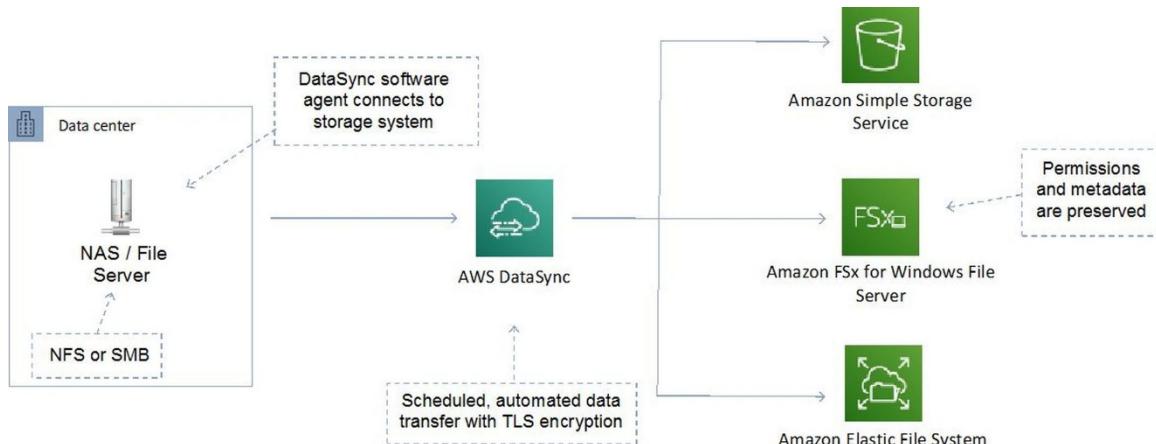
1. Migrate the data to Amazon EFS using the AWS Server Migration Service (SMS)
2. Migrate the data to Amazon FSx for Lustre using AWS DataSync
3. Migrate the data to Amazon FSx for Windows File Server using AWS DataSync
4. Migrate the data to Amazon S3 using and AWS Snowball Edge device

Answer: 3

Explanation:

Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. This is the most suitable destination for this use case.

AWS DataSync can be used to move large amounts of data online between on-premises storage and Amazon S3, Amazon EFS, or Amazon FSx for Windows File Server. The source datastore can be Server Message Block (SMB) file servers.



CORRECT: "Migrate the data to Amazon FSx for Windows File Server using AWS DataSync" is the correct answer.

INCORRECT: "Migrate the data to Amazon EFS using the AWS Server Migration Service (SMS)" is incorrect. EFS is used for hosting filesystems accessed over NFS from Linux (not Windows). The SMS service is used for migrating virtual machines, not data.

INCORRECT: "Migrate the data to Amazon FSx for Lustre using AWS DataSync" is incorrect. Amazon FSx for Windows File Server should be used for hosting SMB shares.

INCORRECT: "Migrate the data to Amazon S3 using and AWS Snowball Edge device" is incorrect. Amazon S3 is an object store and unsuitable for hosting an SMB filesystem. Snowball is not required in this case as the data is not going to S3 and there are no time or bandwidth limitations mentioned in the scenario.

References:

<https://aws.amazon.com/fsx/windows/>

<https://aws.amazon.com/datasync/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-fsx/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-datasync/>

QUESTION 19

The database layer of an on-premises web application is being migrated to AWS. The database uses a multi-threaded, in-memory caching layer to improve performance for repeated queries. Which service would be the most suitable replacement for the database cache?

1. Amazon ElastiCache Redis
2. Amazon DynamoDB DAX
3. Amazon ElastiCache Memcached
4. Amazon RDS MySQL

Answer: 3

Explanation:

Amazon ElastiCache with the Memcached engine is an in-memory database that can be used as a database caching layer. The memcached engine supports multiple cores and threads and large nodes.

	Memcached	Redis (cluster mode disabled)	Redis (cluster mode enabled)
Data types	Simple	Complex	Complex
Data partitioning	Yes	No	Yes
Cluster is modifiable	Yes	Yes	No
Online re-sharding	No	No	3.2.10
Encryption	No	3.2.6	3.2.6
HIPAA Compliance	No	3.2.6	3.2.6
Multi-threaded	Yes	No	No
Node type upgrade	No	Yes	No
Engine upgrading	Yes	Yes	No
High availability (replication)	No	Yes	Yes
Automatic failover	No	Optional	Required

CORRECT: "Amazon ElastiCache Memcached" is the correct answer.

INCORRECT: "Amazon ElastiCache Redis" is incorrect. The Redis engine does not support multiple CPU cores or threads.

INCORRECT: "Amazon DynamoDB DAX" is incorrect. Amazon DynamoDB Accelerator (DAX) is a database cache that should be used with DynamoDB only.

INCORRECT: "Amazon RDS MySQL" is incorrect as this is not an example of an in-memory database that can be used as a database caching layer.

References:

<https://aws.amazon.com/elasticsearch/redis-vs-memcached/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticsearch/>

QUESTION 20

A Solutions Architect is designing an application for processing and extracting data from log files. The log files are generated by an application and the number and frequency of updates varies. The files are up to 1 GB in size and processing will take around 40 seconds for each file.

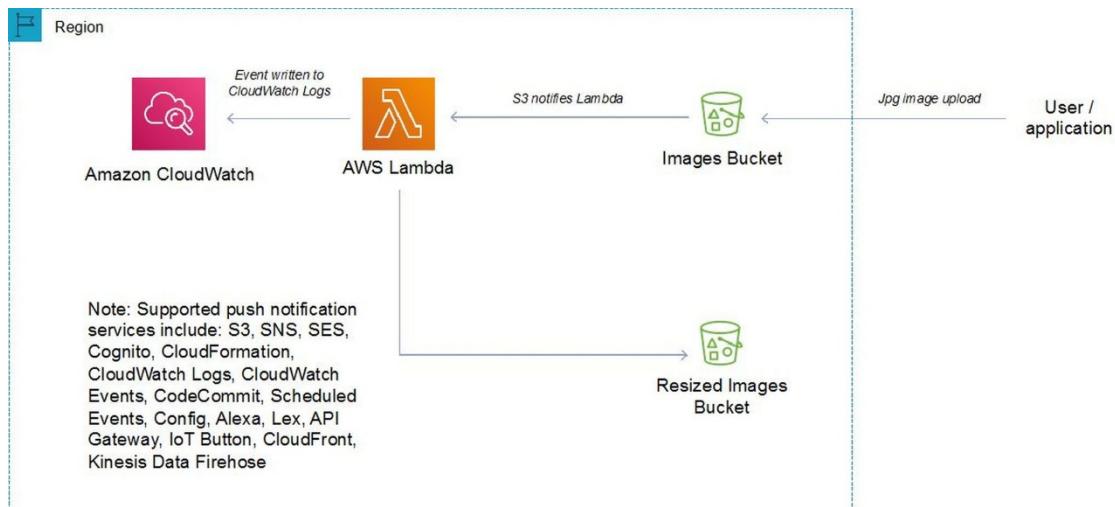
Which solution is the most cost-effective?

1. Write the log files to an Amazon EC2 instance with an attached EBS volume. After processing, save the files to an Amazon S3 bucket
2. Write the log files to an Amazon SQS queue. Use AWS Lambda to process the files from the queue and save to an Amazon S3 bucket
3. Write the log files to an Amazon S3 bucket. Create an event notification to invoke an Amazon ECS task to process the files and save to an Amazon S3 bucket
4. Write the log files to an Amazon S3 bucket. Create an event notification to invoke an AWS Lambda function that will process the files

Answer: 4

Explanation:

The question asks for the most cost-effective solution and therefore a serverless and automated solution will be the best choice. AWS Lambda can run custom code in response to Amazon S3 bucket events. You upload your custom code to AWS Lambda and create a function. When Amazon S3 detects an event of a specific type (for example, an object created event), it can publish the event to AWS Lambda and invoke your function in Lambda. In response, AWS Lambda executes your function.



CORRECT: "Write the log files to an Amazon S3 bucket. Create an event notification to invoke an AWS Lambda function that will process the files" is the correct answer.

INCORRECT: "Write the log files to an Amazon EC2 instance with an attached EBS volume. After processing, save the files to an Amazon S3 bucket" is incorrect. This is not cost effective as it is not serverless.

INCORRECT: "Write the log files to an Amazon SQS queue. Use AWS Lambda to process the files from the queue and save to an Amazon S3 bucket" is incorrect. SQS has a maximum message size of 256 KB so the message body would need to be saved in S3 anyway. Using an event source mapping from S3 would be less complex and preferable.

INCORRECT: "Write the log files to an Amazon S3 bucket. Create an event notification to invoke an Amazon ECS task to process the files and save to an Amazon S3 bucket" is incorrect. You cannot use event notifications to process Amazon ECS tasks.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

QUESTION 21

A large multinational retail company has a presence in AWS in multiple regions. The company has established a new office and needs to implement a high-bandwidth, low-latency connection to multiple VPCs in multiple regions within the same account. The VPCs each have unique CIDR ranges.

What would be the optimum solution design using AWS technology? (Select TWO.)

1. Configure AWS VPN CloudHub
2. Create a Direct Connect gateway, and create private VIFs to each region
3. Provision an MPLS network
4. Implement Direct Connect connections to each AWS region
5. Implement a Direct Connect connection to the closest AWS region

Answer: 2,5

Explanation:

The company should implement an AWS Direct Connect connection to the closest region. A Direct Connect gateway can then be used to create private virtual interfaces (VIFs) to each AWS region.

Direct Connect gateway provides a grouping of Virtual Private Gateways (VGWs) and Private Virtual Interfaces (VIFs) that belong to the same AWS account and enables you to interface with VPCs in any AWS Region (except AWS China Region).

You can share a private virtual interface to interface with more than one Virtual Private Cloud (VPC) reducing the number of BGP sessions required.

CORRECT: "Create a Direct Connect gateway, and create private VIFs to each region" is a correct answer.

CORRECT: "Implement a Direct Connect connection to the closest AWS region" is also a correct answer.

INCORRECT: "Configure AWS VPN CloudHub" is incorrect. AWS VPN CloudHub is not the best solution as you have been asked to implement high-bandwidth, low-latency connections and VPN uses the Internet so is not reliable.

INCORRECT: "Provision an MPLS network" is incorrect. An MPLS network could be used to create a network topology that gets you closer to AWS in each region but you would still need use Direct Connect or VPN for the connectivity into AWS. Also, the question states that you should use AWS technology and MPLS is not offered as a service by AWS.

INCORRECT: "Implement Direct Connect connections to each AWS region" is incorrect. You do not need to implement multiple Direct Connect connections to each region. This would be a more expensive option as you would need to pay for an international private connection.

References:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

QUESTION 22

A Solutions Architect is creating a design for a two-tier application with a MySQL RDS back-end. The performance requirements of the database tier are hard to quantify until the application is running and the Architect is concerned about right-sizing the database.

What methods of scaling are possible after the MySQL RDS database is deployed? (Select TWO.)

1. Vertical scaling for read and write by choosing a larger instance size
2. Horizontal scaling for write capacity by enabling Multi-AZ
3. Vertical scaling for read and write by using Transfer Acceleration

4. Horizontal scaling for read and write by enabling Multi-Master RDS DB
5. Horizontal scaling for read capacity by creating a read-replica

Answer: 1,5

Explanation:

To handle a higher load in your database, you can vertically scale up your master database with a simple push of a button. In addition to scaling your master database vertically, you can also improve the performance of a read-heavy database by using read replicas to horizontally scale your database.

CORRECT: "Vertical scaling for read and write by choosing a larger instance size" is a correct answer.

CORRECT: "Horizontal scaling for read capacity by creating a read-replica" is also a correct answer.

INCORRECT: "Horizontal scaling for write capacity by enabling Multi-AZ" is incorrect. You cannot scale write capacity by enabling Multi-AZ as only one DB is active and can be written to.

INCORRECT: "Vertical scaling for read and write by using Transfer Acceleration" is incorrect. Transfer Acceleration is a feature of S3 for fast uploads of objects.

INCORRECT: "Horizontal scaling for read and write by enabling Multi-Master RDS DB" is incorrect. There is no such thing as a Multi-Master MySQL RDS DB (there is for Aurora).

References:

<https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 23

An application is running on EC2 instances in a private subnet of an Amazon VPC. A Solutions Architect would like to connect the application to Amazon API Gateway. For security reasons, it is necessary to ensure that no traffic traverses the Internet and to ensure all traffic uses private IP addresses only.

How can this be achieved?

1. Create a NAT gateway
2. Create a public VIF on a Direct Connect connection
3. Create a private API using an interface VPC endpoint
4. Add the API gateway to the subnet the EC2 instances are located in

Answer: 3

Explanation:

An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service. Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.

CORRECT: "Create a private API using an interface VPC endpoint" is the correct answer.

INCORRECT: "Create a NAT gateway" is incorrect. NAT Gateways are used to provide Internet access for EC2 instances in private subnets so are of no use in this solution.

INCORRECT: "Create a public VIF on a Direct Connect connection" is incorrect. You do not need to implement Direct Connect and create a public VIF. Public IP addresses are used in public VIFs and the question requests that only private addresses are used.

INCORRECT: "Add the API gateway to the subnet the EC2 instances are located in" is incorrect. You cannot add API Gateway to the subnet the EC2 instances are in, it is a public service with a public endpoint.

References:

<https://aws.amazon.com/blogs/compute/introducing-amazon-api-gateway-private-endpoints/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 24

An application stack is being created which needs a message bus to decouple the application components from each other. The application will generate up to 300 messages per second without using batching. A Solutions Architect needs to ensure that a message is delivered only once and duplicates are not introduced into the queue. It is not necessary to maintain the order of the messages.

Which SQS queue type should be used?

1. Standard queues
2. Long polling queues
3. FIFO queues
4. Auto Scaling queues

Answer: 3

Explanation:

The key fact you need to consider here is that duplicate messages cannot be introduced into the queue. For this reason alone you must use a FIFO queue. The statement about it not being necessary to maintain the order of the messages is meant to confuse you, as that might lead you to think you can use a standard queue, but standard queues don't guarantee that duplicates are not introduced into the queue.

FIFO (first-in-first-out) queues preserve the exact order in which messages are sent and received – note that this is not required in the question but exactly once processing is. FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it.

CORRECT: "FIFO queues" is the correct answer.

INCORRECT: "Standard queues" is incorrect. Standard queues provide a loose-FIFO capability that attempts to preserve the order of messages. Standard queues provide at-least-once delivery, which means that each message is delivered at least once.

INCORRECT: "Long polling queues" is incorrect. Long polling is configuration you can apply to a queue, it is not a queue type.

INCORRECT: "Auto Scaling queues" is incorrect. There is no such thing as an Auto Scaling queue.

References:

<https://aws.amazon.com/sqs/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 25

A Solutions Architect is attempting to clean up unused EBS volumes and snapshots to save some space and cost. How many of the most recent snapshots of an EBS volume need to be maintained to guarantee that you can recreate the full EBS volume from the snapshot?

1. You must retain all snapshots as the process is incremental and therefore data is required from each snapshot
2. Two snapshots, the oldest and most recent snapshots
3. The oldest snapshot, as this references data in all other snapshots
4. Only the most recent snapshot. Snapshots are incremental, but the deletion process will ensure that no data is lost

Answer: 4

Explanation:

Snapshots capture a point-in-time state of an instance. If you make periodic snapshots of a volume, the snapshots are incremental, which means that only the blocks on the device that have changed after your last snapshot are saved in the new snapshot.

Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the volume.

CORRECT: "Only the most recent snapshot. Snapshots are incremental, but the deletion process will ensure that no data is lost" is the correct answer.

INCORRECT: "You must retain all snapshots as the process is incremental and therefore data is required from each snapshot" is

incorrect as explained above.

INCORRECT: "Two snapshots, the oldest and most recent snapshots" is incorrect as explained above.

INCORRECT: "The oldest snapshot, as this references data in all other snapshots" is incorrect as explained above.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-snapshot.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 26

A Python application is currently running on Amazon ECS containers using the Fargate launch type. An ALB has been created with a Target Group that routes incoming connections to the ECS-based application. The application will be used by consumers who will authenticate using federated OIDC compliant Identity Providers such as Google and Facebook. The users must be securely authenticated on the front-end before they access the secured portions of the application.

How can this be configured using an ALB?

1. The only option is to use SAML with Amazon Cognito on the ALB
2. This can be done on the ALB by creating an authentication action on a listener rule that configures an Amazon Cognito user pool with the social IdP
3. This cannot be done on an ALB; you'll need to authenticate users on the back-end with AWS Single Sign-On (SSO) integration
4. This cannot be done on an ALB; you'll need to use another layer in front of the ALB

Answer: 2

Explanation:

ALB supports authentication from OIDC compliant identity providers such as Google, Facebook and Amazon. It is implemented through an authentication action on a listener rule that integrates with Amazon Cognito to create user pools.

SAML can be used with Amazon Cognito but this is not the only option.

CORRECT: "This can be done on the ALB by creating an authentication action on a listener rule that configures an Amazon Cognito user pool with the social IdP" is the correct answer.

INCORRECT: "The only option is to use SAML with Amazon Cognito on the ALB" is incorrect as explained above.

INCORRECT: "This cannot be done on an ALB; you'll need to authenticate users on the back-end with AWS Single Sign-On (SSO) integration" is incorrect as explained above.

INCORRECT: "This cannot be done on an ALB; you'll need to use another layer in front of the ALB" is incorrect as explained above.

References:

<https://aws.amazon.com/blogs/aws/built-in-authentication-in-alb/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 27

A Solutions Architect is creating a solution for an application that must be deployed on Amazon EC2 hosts that are dedicated to the client. Instance placement must be automatic and billing should be per instance.

Which type of EC2 deployment model should be used?

1. Reserved Instance
2. Dedicated Instance
3. Dedicated Host
4. Cluster Placement Group

Answer: 2

Explanation:

Dedicated Instances are Amazon EC2 instances that run in a VPC on hardware that's dedicated to a single customer. Your Dedicated instances are physically isolated at the host hardware level from instances that belong to other AWS accounts. Dedicated instances allow automatic instance placement and billing is per instance.

CORRECT: "Dedicated Instance" is the correct answer.

INCORRECT: "Reserved Instance" is incorrect. Reserved instances are a method of reducing cost by committing to a fixed contract term of 1 or 3 years.

INCORRECT: "Dedicated Host" is incorrect. An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts can help you address compliance requirements and reduce costs by allowing you to use your existing server-bound software licenses. With dedicated hosts billing is on a per-host basis (not per instance).

INCORRECT: "Cluster Placement Group" is incorrect. A Cluster Placement Group determines how instances are placed on underlying hardware to enable low-latency connectivity.

References:

<https://aws.amazon.com/ec2/dedicated-hosts/>

<https://aws.amazon.com/ec2/pricing/dedicated-instances/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 28

There is new requirement for a database that will store a large number of records for an online store. You are evaluating the use of DynamoDB. Which of the following are AWS best practices for DynamoDB? (Select TWO.)

1. Use separate local secondary indexes for each item
2. Store objects larger than 400KB in S3 and use pointers in DynamoDB
3. Store more frequently and less frequently accessed data in separate tables
4. Use for BLOB data use cases
5. Use large files

Answer: 2,3

Explanation:

DynamoDB best practices include:

- Keep item sizes small.
- If you are storing serial data in DynamoDB that will require actions based on data/time use separate tables for days, weeks, months.
- Store more frequently and less frequently accessed data in separate tables.
- If possible compress larger attribute values.
- Store objects larger than 400KB in S3 and use pointers (S3 Object ID) in DynamoDB.

CORRECT: "Store objects larger than 400KB in S3 and use pointers in DynamoDB" is the correct answer.

CORRECT: "Store more frequently and less frequently accessed data in separate tables" is the correct answer.

INCORRECT: "Use separate local secondary indexes for each item" is incorrect as this is not a best practice.

INCORRECT: "Use for BLOB data use cases" is incorrect as this is not a best practice.

INCORRECT: "Use large files" is incorrect as this is not a best practice.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/best-practices.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

QUESTION 29

A Solutions Architect needs to migrate an Oracle database running on RDS onto Amazon RedShift to improve performance and reduce cost. What combination of tasks using AWS services should be followed to execute the migration? (Select TWO.)

1. Migrate the database using the AWS Database Migration Service (DMS)
2. Convert the schema using the AWS Schema Conversion Tool
3. Take a snapshot of the Oracle database and restore the snapshot onto RedShift
4. Configure API Gateway to extract, transform and load the data into RedShift
5. Enable log shipping from the Oracle database to RedShift

Answer: 1,2

Explanation:

Convert the data warehouse schema and code from the Oracle database running on RDS using the AWS Schema Conversion Tool (AWS SCT) then migrate data from the Oracle database to Amazon Redshift using the AWS Database Migration Service (AWS DMS)

CORRECT: "Migrate the database using the AWS Database Migration Service (DMS)" is the correct answer.

CORRECT: "Convert the schema using the AWS Schema Conversion Tool" is the correct answer.

INCORRECT: "Take a snapshot of the Oracle database and restore the snapshot onto RedShift" is incorrect. Snapshots are not a supported migration method from RDS to RedShift.

INCORRECT: "Configure API Gateway to extract, transform and load the data into RedShift" is incorrect. API Gateway is not used for ETL functions.

INCORRECT: "Enable log shipping from the Oracle database to RedShift" is incorrect. Log shipping is not a supported migration method from RDS to RedShift.

References:

<https://aws.amazon.com/getting-started/projects/migrate-oracle-to-amazon-redshift/>

QUESTION 30

A client has made some updates to their web application. The application uses an Auto Scaling Group to maintain a group of several EC2 instances. The application has been modified and a new AMI must be used for launching any new instances.

What does a Solutions Architect need to do to add the new AMI?

1. Create a new target group that uses a new launch configuration with the new AMI
2. Modify the existing launch configuration to add the new AMI
3. Suspend Auto Scaling and replace the existing AMI
4. Create a new launch configuration that uses the AMI and update the ASG to use the new launch configuration

Answer: 4

Explanation:

A launch configuration is the template used to create new EC2 instances and includes parameters such as instance family, instance type, AMI, key pair and security groups.

You cannot edit a launch configuration once defined. In this case you can create a new launch configuration that uses the new AMI and any new instances that are launched by the ASG will use the new AMI.

CORRECT: "Create a new launch configuration that uses the AMI and update the ASG to use the new launch configuration" is the correct answer.

INCORRECT: "Create a new target group that uses a new launch configuration with the new AMI" is incorrect. A target group is a concept associated with an ELB not Auto Scaling.

INCORRECT: "Modify the existing launch configuration to add the new AMI" is incorrect as you cannot modify an existing launch configuration.

INCORRECT: "Suspend Auto Scaling and replace the existing AMI" is incorrect. Suspending scaling processes can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes. It is not useful in this situation.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html>

Save time with our exam-specific cheat sheets:

QUESTION 31

A Solutions Architect regularly deploys and manages infrastructure services for customers on AWS. The SysOps team are facing challenges in tracking changes that are made to the infrastructure services and rolling back when problems occur.

How can a Solutions Architect BEST assist the SysOps team?

1. Use AWS Systems Manager to manage all updates to the infrastructure services
2. Use CodeDeploy to manage version control for the infrastructure services
3. Use CloudFormation templates to deploy and manage the infrastructure services
4. Use Trusted Advisor to record updates made to the infrastructure services

Answer: 3

Explanation:

When you provision your infrastructure with AWS CloudFormation, the AWS CloudFormation template describes exactly what resources are provisioned and their settings. Because these templates are text files, you simply track differences in your templates to track changes to your infrastructure, similar to the way developers control revisions to source code.

For example, you can use a version control system with your templates so that you know exactly what changes were made, who made them, and when. If at any point you need to reverse changes to your infrastructure, you can use a previous version of your template.

CORRECT: "Use CloudFormation templates to deploy and manage the infrastructure services" is the correct answer.

INCORRECT: "Use AWS Systems Manager to manage all updates to the infrastructure services" is incorrect. AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. However, CloudFormation would be the preferred method of maintaining the state of the overall architecture.

INCORRECT: "Use CodeDeploy to manage version control for the infrastructure services" is incorrect. AWS CodeDeploy is a deployment service that automates application (not infrastructure) deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda functions. This would be a good fit if we were talking about an application environment where code changes need to be managed but not for infrastructure services..

INCORRECT: "Use Trusted Advisor to record updates made to the infrastructure services" is incorrect. AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.

References:

<https://aws.amazon.com/cloudformation/resources/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 32

A Solutions Architect is designing the compute layer of a serverless application. The compute layer will manage requests from external systems, orchestrate serverless workflows, and execute the business logic.

The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the compute layer? (Select TWO.)

1. Use Amazon ECS for executing the business logic
2. Use AWS CloudFormation for orchestrating serverless workflows
3. Use AWS Step Functions for orchestrating serverless workflows
4. Use AWS Elastic Beanstalk for executing the business logic
5. Use Amazon API Gateway with AWS Lambda for executing the business logic

Answer: 3,5

Explanation:

With Amazon API Gateway, you can run a fully managed REST API that integrates with Lambda to execute your business logic

and includes traffic management, authorization and access control, monitoring, and API versioning.

AWS Step Functions orchestrates serverless workflows including coordination, state, and function chaining as well as combining long-running executions not supported within Lambda execution limits by breaking into multiple steps or by calling workers running on Amazon Elastic Compute Cloud (Amazon EC2) instances or on-premises.

CORRECT: "Use AWS Step Functions for orchestrating serverless workflows" is the correct answer.

CORRECT: "Use Amazon API Gateway with AWS Lambda for executing the business logic" is the correct answer.

INCORRECT: "Use Amazon ECS for executing the business logic" is incorrect. The Amazon Elastic Container Service (ECS) is not a serverless application stack, containers run on EC2 instances.

INCORRECT: "Use AWS CloudFormation for orchestrating serverless workflows" is incorrect. AWS CloudFormation is used for describing and provisioning resources not actually performing workflow functions within the application.

INCORRECT: "Use AWS Elastic Beanstalk for executing the business logic" is incorrect. AWS Elastic Beanstalk is used for describing and provisioning resources not actually performing workflow functions within the application.

References:

<https://aws.amazon.com/step-functions/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/>

QUESTION 33

An application running in an on-premise data center writes data to a MySQL database. A Solutions Architect is re-architecting the application and plans to move the database layer into the AWS cloud on Amazon RDS. The application layer will run in the on-premise data center.

What must be done to connect the application to the RDS database via the Internet? (Select TWO.)

1. Configure a NAT Gateway and attach the RDS database
2. Choose to make the RDS instance publicly accessible and place it in a public subnet
3. Select a public IP within the DB subnet group to assign to the RDS instance
4. Create a security group allowing access from the on-premise public IP to the RDS instance and assign to the RDS instance
5. Create a DB subnet group that is publicly accessible

Answer: 2,4

Explanation:

When you create the RDS instance, you need to select the option to make it publicly accessible. A security group will need to be created and assigned to the RDS instance to allow access from the public IP address of your application (or firewall).

CORRECT: "Choose to make the RDS instance publicly accessible and place it in a public subnet" is a correct answer.

CORRECT: "Create a security group allowing access from the on-premise public IP to the RDS instance and assign to the RDS instance" is also a correct answer.

INCORRECT: "Configure a NAT Gateway and attach the RDS database" is incorrect. NAT Gateways are used for enabling Internet connectivity for EC2 instances in private subnets.

INCORRECT: "Select a public IP within the DB subnet group to assign to the RDS instance" is incorrect. The RDS instance does not require a public IP.

INCORRECT: "Create a DB subnet group that is publicly accessible" is incorrect. A DB subnet group is a collection of subnets (typically private) that you create in a VPC and that you then designate for your DB instance. The DB subnet group cannot be made publicly accessible, even if the subnets are public subnets, it is the RDS DB that must be configured to be publicly accessible.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html#USER_VPC.Scenario4

Save time with our exam-specific cheat sheets:

QUESTION 34

A Solutions Architect is conducting an audit and needs to query several properties of EC2 instances in a VPC. Which two methods are available for accessing and querying the properties of an EC2 instance such as instance ID, public keys and network interfaces? (Select TWO.)

1. Use the EC2 Config service
2. Run the command "curl http://169.254.169.254/latest/meta-data/"
3. Download and run the Instance Metadata Query Tool
4. Run the command "curl http://169.254.169.254/latest/dynamic/instance-identity/"
5. Use the Batch command

Answer: 2,3

Explanation:

This information is stored in the instance metadata on the instance. You can access the instance metadata through a URI or by using the Instance Metadata Query tool.

The instance metadata is available at <http://169.254.169.254/latest/meta-data>.

The Instance Metadata Query tool allows you to query the instance metadata without having to type out the full URI or category names.

CORRECT: "Run the command "curl http://169.254.169.254/latest/meta-data/"" is a correct answer.

CORRECT: "Download and run the Instance Metadata Query Tool" is also a correct answer.

INCORRECT: "Use the EC2 Config service" is incorrect. The EC2 config is not suitable for accessing this information.

INCORRECT: "Run the command "curl http://169.254.169.254/latest/dynamic/instance-identity/"" is incorrect. The correct command is provided above.

INCORRECT: "Use the Batch command" is incorrect. The batch command is not suitable for accessing this information.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 35

Encrypted Amazon Elastic Block Store (EBS) volumes are attached to some Amazon EC2 instances. Which statements are correct about using encryption with Amazon EBS volumes? (Select TWO.)

1. Data is only encrypted at rest
2. Encryption is supported on all Amazon EBS volume types
3. Data in transit between an instance and an encrypted volume is also encrypted
4. Volumes created from encrypted snapshots are unencrypted
5. You cannot mix encrypted with unencrypted volumes on an instance

Answer: 2,3

Explanation:

Some facts about Amazon EBS encrypted volumes and snapshots:

- All **EBS** types support encryption and all instance **families** now support encryption.
- Not all **instance** types support encryption.
- Data in transit between an instance and an encrypted volume is also encrypted (data is encrypted in trans).
- You can have encrypted and unencrypted EBS volumes attached to an instance at the same time.
- Snapshots of encrypted volumes are encrypted automatically.
- EBS volumes restored from encrypted snapshots are encrypted automatically.
- EBS volumes created from encrypted snapshots are also encrypted.

CORRECT: "Encryption is supported on all Amazon EBS volume types" is a correct answer.

CORRECT: "Data in transit between an instance and an encrypted volume is also encrypted" is also a correct answer.

INCORRECT: "Data is only encrypted at rest" is incorrect. Please refer to the facts above.

INCORRECT: "Volumes created from encrypted snapshots are unencrypted" is incorrect. Please refer to the facts above.

INCORRECT: "You cannot mix encrypted with unencrypted volumes on an instance" is incorrect. Please refer to the facts above.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 36

An operations team would like to be notified if an RDS database exceeds certain metric thresholds. How can a Solutions Architect automate this process for the operations team?

1. Create a CloudWatch alarm and associate an SQS queue with it that delivers a message to SES
2. Setup an RDS alarm and associate an SNS topic with it that sends an email
3. Create a CloudTrail alarm and configure a notification event to send an SMS
4. Create a CloudWatch alarm and associate an SNS topic with it that sends an email notification

Answer: 4

Explanation:

You can create a CloudWatch alarm that watches a single CloudWatch metric or the result of a math expression based on CloudWatch metrics. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods.

The action can be an Amazon EC2 action, an Amazon EC2 Auto Scaling action, or a notification sent to an Amazon SNS topic. SNS can be configured to send an email notification

CORRECT: "Create a CloudWatch alarm and associate an SNS topic with it that sends an email notification" is the correct answer.

INCORRECT: "Create a CloudWatch alarm and associate an SQS queue with it that delivers a message to SES" is incorrect. You cannot associate an SQS queue with a CloudWatch alarm.

INCORRECT: "Setup an RDS alarm and associate an SNS topic with it that sends an email" is incorrect. CloudWatch performs performance monitoring so you don't setup alarms in RDS itself.

INCORRECT: "Create a CloudTrail alarm and configure a notification event to send an SMS" is incorrect. CloudTrail is used for auditing API access, not for performance monitoring.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/>

QUESTION 37

An Amazon VPC contains a mixture of Amazon EC2 instances in production and non-production environments. A Solutions Architect needs to devise a way to segregate access permissions to different sets of users for instances in different environments.

How can this be achieved? (Select TWO.)

1. Attach an Identity Provider (IdP) and delegate access to the instances to the relevant groups
2. Create an IAM policy that grants access to any instances with the specific tag and attach to the users and groups
3. Create an IAM policy with a conditional statement that matches the environment variables
4. Add an environment variable to the instances using user data
5. Add a specific tag to the instances you want to grant the users or groups access to

Answer: 2,5

Explanation:

You can use the condition checking in IAM policies to look for a specific tag. IAM checks that the tag attached to the principal making the request matches the specified key name and value.

CORRECT: "Create an IAM policy that grants access to any instances with the specific tag and attach to the users and groups" is the correct answer.

CORRECT: "Add a specific tag to the instances you want to grant the users or groups access to" is the correct answer.

INCORRECT: "Attach an Identity Provider (IdP) and delegate access to the instances to the relevant groups" is incorrect. You cannot use an IdP for this solution.

INCORRECT: "Create an IAM policy with a conditional statement that matches the environment variables" is incorrect as the statement should be checking for the tag.

INCORRECT: "Add an environment variable to the instances using user data" is incorrect. You cannot achieve this outcome using environment variables stored in user data and conditional statements in a policy. You must use an IAM policy that grants access to instances based on the tag.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/iam-ec2-resource-tags/>

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

QUESTION 38

A customer runs an application on-premise that stores large media files. The data is mounted to different servers using either the SMB or NFS protocols. The customer is having issues with scaling the storage infrastructure on-premise and is looking for a way to offload the data set into the cloud whilst retaining a local cache for frequently accessed content.

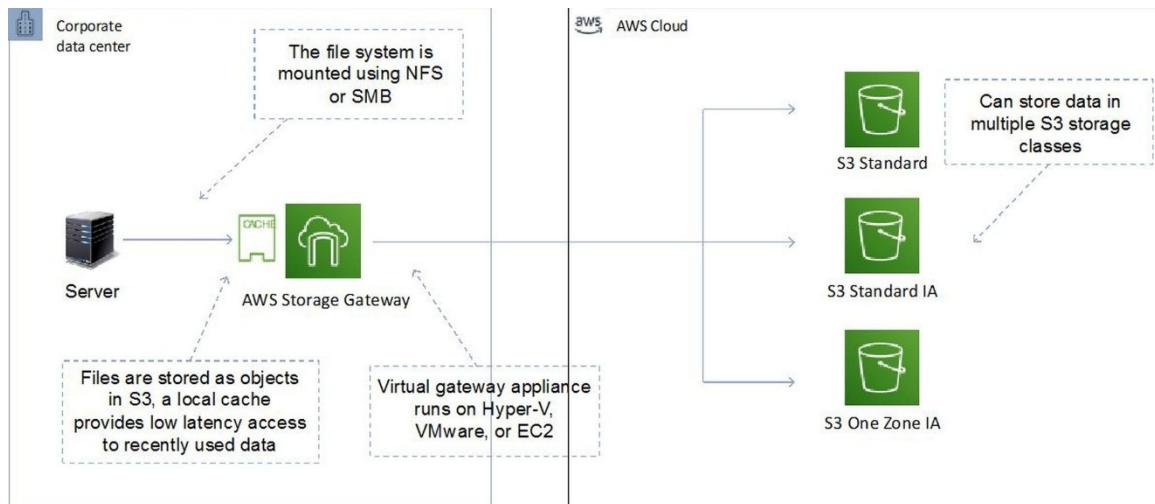
Which of the following is the best solution?

1. Use the AWS Storage Gateway File Gateway
2. Use the AWS Storage Gateway Volume Gateway in cached volume mode
3. Create a script that migrates infrequently used data to S3 using multi-part upload
4. Establish a VPN and use the Elastic File System (EFS)

Answer: 1

Explanation:

File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2-resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.



CORRECT: "Use the AWS Storage Gateway File Gateway" is the correct answer.

INCORRECT: "Use the AWS Storage Gateway Volume Gateway in cached volume mode" is incorrect. The AWS Storage Gateway Volume Gateway in cached volume mode is a block-based (not file-based) solution so you cannot mount the storage with the SMB or NFS protocols. With Cached Volume mode – the entire dataset is stored on S3 and a cache of the most frequently accessed data is cached on-site.

INCORRECT: "Create a script that migrates infrequently used data to S3 using multi-part upload" is incorrect. Creating a script that migrates infrequently used data to S3 is possible but that data would then not be indexed on the primary filesystem so you wouldn't have a method of retrieving it without developing some code to pull it back from S3. This is not the best solution.

INCORRECT: "Establish a VPN and use the Elastic File System (EFS)" is incorrect. You could mount EFS over a VPN but it would not provide you a local cache of the data.

References:

<https://aws.amazon.com/storagegateway/file/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/>

QUESTION 39

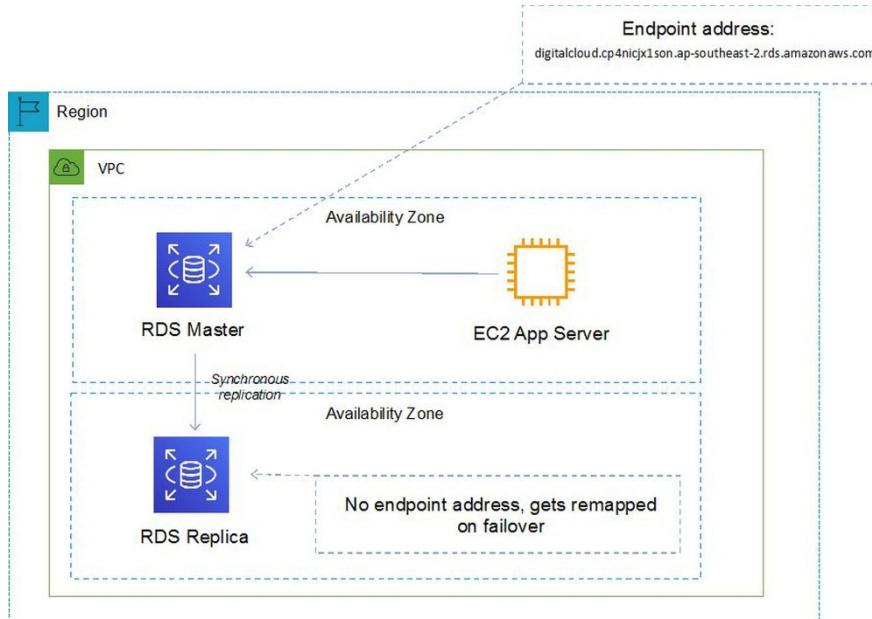
A client has requested a design for a fault tolerant database that can failover between AZs. You have decided to use RDS in a multi-AZ configuration. What type of replication will the primary database use to replicate to the standby instance?

1. Continuous replication
2. Asynchronous replication
3. Scheduled replication
4. Synchronous replication

Answer: 4

Explanation:

Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it (DR only). Multi-AZ deployments for the MySQL, MariaDB, Oracle and PostgreSQL engines utilize synchronous physical replication. Multi-AZ deployments for the SQL Server engine use synchronous logical replication (SQL Server-native Mirroring technology).



CORRECT: "Synchronous replication" is the correct answer.

INCORRECT: "Continuous replication" is incorrect. Continuous replication is not a replication type that is supported by RDS.

INCORRECT: "Asynchronous replication" is incorrect. Asynchronous replication is used by RDS for Read Replicas.

INCORRECT: "Scheduled replication" is incorrect. Scheduled replication is not a replication type that is supported by RDS.

References:

<https://aws.amazon.com/rds/features/multi-az/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 40

A Solutions Architect needs a storage solution for a fleet of Linux web application servers. The solution should provide a file system interface and be able to support millions of files. Which AWS service should the Architect choose?

1. Amazon ElastiCache
2. Amazon EBS
3. Amazon EFS
4. Amazon S3

Answer: 3

Explanation:

The Amazon Elastic File System (EFS) is the only storage solution in the list that provides a file system interface. It also supports millions of files as requested.

CORRECT: "Amazon EFS" is the correct answer.

INCORRECT: "Amazon ElastiCache" is incorrect. Amazon ElastiCache is an in-memory caching solution for databases.

INCORRECT: "Amazon EBS" is incorrect. Amazon EBS provides a block storage interface.

INCORRECT: "Amazon S3" is incorrect. Amazon S3 is an object storage solution and does not provide a file system interface.

References:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 41

A Solutions Architect is creating an application design with several components that will be publicly addressable. The Architect would like to use Alias records. Using Route 53 Alias records what targets can you specify? (Select TWO.)

1. CloudFront distribution
2. ElastiCache cluster
3. EFS filesystems
4. Elastic Beanstalk environment
5. On-premise web server

Answer: 1,4

Explanation:

Alias records are used to map resource record sets in your hosted zone to Amazon Elastic Load Balancing load balancers, API Gateway custom regional APIs and edge-optimized APIs, CloudFront Distributions, AWS Elastic Beanstalk environments, Amazon S3 buckets that are configured as website endpoints, Amazon VPC interface endpoints, and to other records in the same Hosted Zone.

CORRECT: "CloudFront distribution" is the correct answer.

CORRECT: "Elastic Beanstalk environment" is the correct answer.

INCORRECT: "ElastiCache cluster" is incorrect. You cannot use an Alias to point at an ElastiCache cluster or VPC endpoint.

INCORRECT: "EFS filesystems" is incorrect. You cannot use an Alias to point to an EFS filesystem.

INCORRECT: "On-premise web server" is incorrect. You cannot point an Alias record directly at an on-premises web server (you can point to another record in a hosted zone, which could point to an on-premises web server though I'm not sure if this is

supported).

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

QUESTION 42

A new financial platform has been re-architected to use Docker containers in a micro-services architecture. The new architecture will be implemented on AWS and a Solutions Architect must recommend the solution configuration. For operational reasons, it will be necessary to access the operating system of the instances on which the containers run.

Which solution delivery option should the Architect select?

1. ECS with the EC2 launch type
2. EKS with Kubernetes managed infrastructure
3. ECS with the Fargate launch type
4. ECS with a default cluster

Answer: 1

Explanation:

Amazon Elastic Container Service (ECS) is a highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances

The EC2 Launch Type allows you to run containers on EC2 instances that you manage so you will be able to access the operating system instances.

CORRECT: "ECS with the EC2 launch type" is the correct answer.

INCORRECT: "EKS with Kubernetes managed infrastructure" is incorrect. The EKS service is a managed Kubernetes service that provides a fully-managed control plane so you would not have access to the EC2 instances that the platform runs on.

INCORRECT: "ECS with the Fargate launch type" is incorrect. The Fargate Launch Type is a serverless infrastructure managed by AWS so you do not have access to the operating system of the EC2 instances that the container platform runs on.

INCORRECT: "ECS with a default cluster" is incorrect. You need to choose the launch type to ensure you get the access required, not the cluster configuration.

References:

<https://aws.amazon.com/ecs/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

QUESTION 43

A new application runs on Amazon EC2 instances and uses API Gateway and AWS Lambda. The company is planning on running an advertising campaign that will likely result in significant hits to the application after each ad is run.

A Solutions Architect is concerned about the impact this may have on the application and would like to put in place some controls to limit the number of requests per second that hit the application.

What controls should the Solutions Architect implement?

1. Implement throttling rules on the API Gateway
2. Enable caching on the API Gateway and specify a size in gigabytes
3. Enable Lambda continuous scaling
4. API Gateway and Lambda scale automatically to handle any load so there's no need to implement controls

Answer: 1

Explanation:

The key requirement is to limit the number of requests per second that hit the application. This can only be done by

implementing throttling rules on the API Gateway. Throttling enables you to throttle the number of requests to your API which in turn means less traffic will be forwarded to your application server.

CORRECT: "Implement throttling rules on the API Gateway" is the correct answer.

INCORRECT: "Enable caching on the API Gateway and specify a size in gigabytes" is incorrect. Caching can improve performance but does not limit the amount of requests coming in.

INCORRECT: "Enable Lambda continuous scaling" is incorrect. Lambda continuous scaling does not resolve the scalability concerns with the EC2 application server.

INCORRECT: "API Gateway and Lambda scale automatically to handle any load so there's no need to implement controls" is incorrect. API Gateway and Lambda both scale up to their default limits however the bottleneck is with the application server running on EC2 which may not be able to scale to keep up with demand.

References:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/>

QUESTION 44

A Solutions Architect has deployed a number of AWS resources using CloudFormation. Some changes must be made to a couple of resources within the stack. Due to recent failed updates, the Solutions Architect is a little concerned about the effects that implementing updates to the resources might have on other resources in the stack.

What is the easiest way to proceed cautiously?

1. Create and execute a change set
2. Use OpsWorks to manage the configuration changes
3. Use a direct update
4. Deploy a new stack to test the changes

Answer: 1

Explanation:

AWS CloudFormation provides two methods for updating stacks: direct update or creating and executing change sets. When you directly update a stack, you submit changes and AWS CloudFormation immediately deploys them.

Use direct updates when you want to quickly deploy your updates. With change sets, you can preview the changes AWS CloudFormation will make to your stack, and then decide whether to apply those changes.

CORRECT: "Create and execute a change set" is the correct answer.

INCORRECT: "Use OpsWorks to manage the configuration changes" is incorrect. You cannot use OpsWorks to manage the configuration changes. OpsWorks is used for implementing managed Chef and Puppet services.

INCORRECT: "Use a direct update" is incorrect. Direct updates will not provide the safeguard of being able to preview the changes as changes sets do.

INCORRECT: "Deploy a new stack to test the changes" is incorrect. You do not need to go to the trouble and cost of deploying a new stack.

References:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/>

QUESTION 45

A company has over 2000 users and is planning to migrate data into the AWS Cloud. Some of the data is user's home folders on an existing file share and the plan is to move this data to Amazon S3. Each user will have a folder in a shared bucket under the folder structure: *bucket/home/%username%*.

What steps should a Solutions Architect take to ensure that each user can access their own home folder and no one else's? (Select TWO.)

1. Create a bucket policy that applies access permissions based on username
2. Create an IAM policy that applies folder-level permissions
3. Create an IAM policy that applies object-level S3 ACLs
4. Attach an S3 ACL sub-resource that grants access based on the %username% variable
5. Create an IAM group and attach the IAM policy, add IAM users to the group

Answer: 2,5

Explanation:

The AWS blog URL below explains how to construct an IAM policy for a similar scenario. Please refer to the article for detailed instructions.

CORRECT: "Create an IAM policy that applies folder-level permissions" is a correct answer.

CORRECT: "Create an IAM group and attach the IAM policy, add IAM users to the group" is also a correct answer.

INCORRECT: "Create a bucket policy that applies access permissions based on username" is incorrect. An IAM policy rather than a bucket policy should be used.

INCORRECT: "Create an IAM policy that applies object-level S3 ACLs" is incorrect as this cannot be done through an IAM policy.

INCORRECT: "Attach an S3 ACL sub-resource that grants access based on the %username% variable" is incorrect as an IAM policy should be used to control access.

References:

<https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 46

An event in CloudTrail is the record of an activity in an AWS account. What are the two types of events that can be logged in CloudTrail? (Select TWO.)

1. Platform Events which are also known as hardware level operations
2. Data Events which are also known as data plane operations
3. System Events which are also known as instance level operations
4. Control Events which are also known as data plane operations
5. Management Events which are also known as control plane operations

Answer: 2,5

Explanation:

Trails can be configured to log Data events and management events:

Data events: These events provide insight into the resource operations performed on or within a resource. These are also known as data plane operations

Management events: Management events provide insight into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account

CORRECT: "Data Events which are also known as data plane operations" is a correct answer.

CORRECT: "Management Events which are also known as control plane operations" is also a correct answer.

INCORRECT: "Platform Events which are also known as hardware level operations" is incorrect as this not a valid event type.

INCORRECT: "System Events which are also known as instance level operations" is incorrect as this not a valid event type.

INCORRECT: "Control Events which are also known as data plane operations" is incorrect as this not a valid event type.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-management-and-data-events-with-cloudtrail.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudtrail/>

QUESTION 47

A Solutions Architect is writing some code that uses an AWS Lambda function and would like to enable the function to connect to an Amazon ElastiCache cluster within an Amazon VPC in the same AWS account. What VPC-specific information must be included in the function to enable this configuration? (Select TWO.)

1. VPC Subnet IDs
2. VPC Logical IDs
3. VPC Peering IDs
4. VPC Security Group IDs
5. VPC Route Table IDs

Answer: 1,4

Explanation:

To enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs. AWS Lambda uses this information to set up elastic network interfaces (ENIs) that enable your function.

Please see the AWS article linked below for more details on the requirements

CORRECT: "VPC Subnet IDs" is the correct answer.

CORRECT: "VPC Security Group IDs" is the correct answer.

INCORRECT: "VPC Logical IDs" is incorrect as this is not required.

INCORRECT: "VPC Peering IDs" is incorrect as this is not required.

INCORRECT: "VPC Route Table IDs" is incorrect as this is not required.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/vpc.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

QUESTION 48

A Solutions Architect created a new subnet in an Amazon VPC and launched an Amazon EC2 instance into it. The Solutions Architect needs to directly access the EC2 instance from the Internet and cannot connect. Which steps should be undertaken to troubleshoot the issue? (Select TWO.)

1. Check that the instance has a public IP address
2. Check that there is a NAT Gateway configured for the subnet
3. Check that Security Group has a rule for outbound traffic
4. Check that the route table associated with the subnet has an entry for an Internet Gateway
5. Check that you can ping the instance from another subnet

Answer: 1,4

Explanation:

A public subnet is a subnet that's associated with a route table that has a route to an Internet gateway.

Public subnets are subnets that have:

- "Auto-assign public IPv4 address" set to "Yes".
- The subnet route table has an attached Internet Gateway.

CORRECT: "Check that the instance has a public IP address" is the correct answer.

CORRECT: "Check that the route table associated with the subnet has an entry for an Internet Gateway" is the correct answer.

INCORRECT: "Check that there is a NAT Gateway configured for the subnet" is incorrect. A NAT Gateway is used for providing outbound Internet access for EC2 instances in private subnets.

INCORRECT: "Check that Security Group has a rule for outbound traffic" is incorrect. Security groups are stateful and do not need a rule for outbound traffic. For this solution you would only need to create an inbound rule that allows the relevant protocol.

INCORRECT: "Check that you can ping the instance from another subnet" is incorrect. Checking you can ping from another subnet does not relate to being able to access the instance remotely as it uses different protocols and a different network path.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 49

A Solutions Architect just completed the implementation of a 2-tier web application for a client. The application uses Amazon EC2 instances, Amazon ELB and Auto Scaling across two subnets. After deployment the Solutions Architect noticed that only one subnet has EC2 instances running in it. What might be the cause of this situation?

1. The ELB is configured as an internal-only load balancer
2. The Auto Scaling Group has not been configured with multiple subnets
3. Cross-zone load balancing is not enabled on the ELB
4. The AMI is missing from the ASG's launch configuration

Answer: 2

Explanation:

You can specify which subnets Auto Scaling will launch new instances into. Auto Scaling will try to distribute EC2 instances evenly across AZs. If only one subnet has EC2 instances running in it the first thing to check is that you have added all relevant subnets to the configuration.

CORRECT: "The Auto Scaling Group has not been configured with multiple subnets" is the correct answer.

INCORRECT: "The ELB is configured as an internal-only load balancer" is incorrect. The type of ELB deployed is not relevant here as Auto Scaling is responsible for launching instances into subnets whereas ELB is responsible for distributing connections to the instances.

INCORRECT: "Cross-zone load balancing is not enabled on the ELB" is incorrect. Cross-zone load balancing is an ELB feature and ELB is not the issue here as it is not responsible for launching instances into subnets.

INCORRECT: "The AMI is missing from the ASG's launch configuration" is incorrect. If the AMI was missing from the launch configuration no instances would be running.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-in-vpc.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 50

A Solutions Architect is designing the messaging and streaming layers of a serverless application. The messaging layer will manage communications between components and the streaming layer will manage real-time analysis and processing of streaming data.

The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the messaging and streaming layers? (Select TWO.)

1. Use Amazon Kinesis for collecting, processing and analyzing real-time streaming data
2. Use Amazon SWF for providing a fully managed messaging service
3. Use Amazon SNS for providing a fully managed messaging service
4. Use Amazon EMR for collecting, processing and analyzing real-time streaming data
5. Use AWS CloudTrail for collecting, processing and analyzing real-time streaming data

Answer: 1,3**Explanation:**

Amazon Kinesis makes it easy to collect, process, and analyze real-time streaming data. With Amazon Kinesis Analytics, you can run standard SQL or build entire streaming applications using SQL.

Amazon Simple Notification Service (Amazon SNS) provides a fully managed messaging service for pub/sub patterns using asynchronous event notifications and mobile push notifications for microservices, distributed systems, and serverless applications.

CORRECT: "Use Amazon Kinesis for collecting, processing and analyzing real-time streaming data" is the correct answer.

CORRECT: "Use Amazon SNS for providing a fully managed messaging service" is the correct answer.

INCORRECT: "Use Amazon SWF for providing a fully managed messaging service" is incorrect. Amazon Simple Workflow Service is used for executing tasks not sending messages.

INCORRECT: "Use Amazon EMR for collecting, processing and analyzing real-time streaming data" is incorrect. Amazon Elastic Map Reduce runs on EC2 instances so is not serverless.

INCORRECT: "Use AWS CloudTrail for collecting, processing and analyzing real-time streaming data" is incorrect. AWS CloudTrail is used for recording API activity on your account.

References:

<https://aws.amazon.com/kinesis/>

<https://aws.amazon.com/sns/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/>

QUESTION 51

An existing Auto Scaling group is running with eight Amazon EC2 instances. A Solutions Architect has attached an Elastic Load Balancer (ELB) to the Auto Scaling group by connecting a Target Group. The ELB is in the same region and already has ten EC2 instances running in the Target Group.

When attempting to attach the ELB the request immediately fails, what is the MOST likely cause?

1. Adding the 10 EC2 instances to the ASG would exceed the maximum capacity configured
2. One or more of the instances are unhealthy
3. ASGs cannot be edited once defined, you would need to recreate it
4. You cannot attach running EC2 instances to an ASG

Answer: 1**Explanation:**

You can attach one or more Target Groups to your ASG to include instances behind an ALB and the ELBs must be in the same region. Once you do this any EC2 instance existing or added by the ASG will be automatically registered with the ASG defined ELBs. If adding an instance to an ASG would result in exceeding the maximum capacity of the ASG the request will fail.

CORRECT: "Adding the 10 EC2 instances to the ASG would exceed the maximum capacity configured" is the correct answer.

INCORRECT: "One or more of the instances are unhealthy" is incorrect. After the load balancer enters the InService state, Amazon EC2 Auto Scaling terminates and replaces any instances that are reported as unhealthy. However, in this case the request immediately failed so having one or more unhealthy instances is not the issue.

INCORRECT: "ASGs cannot be edited once defined, you would need to recreate it" is incorrect. Auto Scaling Groups can be edited once created (however launch configurations cannot be edited).

INCORRECT: "You cannot attach running EC2 instances to an ASG" is incorrect. You can attach running EC2 instances to an ASG.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html>

Save time with our exam-specific cheat sheets:

QUESTION 52

The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. According to the policy, what is AWS's position on penetration testing?

1. AWS do not allow any form of penetration testing
2. AWS allow penetration testing by customers on their own VPC resources
3. AWS allow penetration for some resources without prior authorization
4. AWS allow penetration testing for all resources

Answer: 3

Explanation:

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services. Please check the AWS link below for the latest information.

CORRECT: "AWS allow penetration for some resources without prior authorization" is the correct answer.

INCORRECT: "AWS do not allow any form of penetration testing" is incorrect as explained above.

INCORRECT: "AWS allow penetration testing by customers on their own VPC resources" is incorrect as explained above.

INCORRECT: "AWS allow penetration testing for all resources" is incorrect as explained above.

References:

<https://aws.amazon.com/security/penetration-testing/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-certified-cloud-practitioner/cloud-security/>

QUESTION 53

An application regularly uploads files from an Amazon EC2 instance to an Amazon S3 bucket. The files can be a couple of gigabytes in size and sometimes the uploads are slower than desired. What method can be used to increase throughput and reduce upload times?

1. Turn off versioning on the destination bucket
2. Randomize the object names when uploading
3. Use Amazon S3 multipart upload
4. Upload the files using the S3 Copy SDK or REST API

Answer: 3

Explanation:

Multipart upload can be used to speed up uploads to S3. Multipart upload uploads objects in parts independently, in parallel and in any order. It is performed using the S3 Multipart upload API and is recommended for objects of 100MB or larger. It can be used for objects from 5MB up to 5TB and must be used for objects larger than 5GB.

CORRECT: "Use Amazon S3 multipart upload" is the correct answer.

INCORRECT: "Turn off versioning on the destination bucket" is incorrect. Turning off versioning will not speed up the upload.

INCORRECT: "Randomize the object names when uploading" is incorrect. Randomizing object names provides no value in this context, random prefixes are used for intensive read requests.

INCORRECT: "Upload the files using the S3 Copy SDK or REST API" is incorrect. Copy is used for copying, moving and renaming objects within S3 not for uploading to S3.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 54

A three-tier web application that is deployed in an Amazon VPC has been experiencing heavy load on the database layer. The database layer uses an Amazon RDS MySQL instance in a multi-AZ configuration. Customers have been complaining about poor response times. During troubleshooting it has been noted that the database layer is experiencing high read contention during peak hours of the day.

What are two possible options that could be used to offload some of the read traffic from the database to resolve the performance issues? (Select TWO.)

1. Add RDS read replicas in each AZ
2. Use an ELB to distribute load between RDS instances
3. Migrate to DynamoDB
4. Use a larger RDS instance size
5. Deploy ElastiCache in each AZ

Answer: 1,5

Explanation:

Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads.

Read replicas are used for read heavy DBs and replication is asynchronous. They are for workload sharing and offloading and are created from a snapshot of the master instance

CORRECT: "Add RDS read replicas in each AZ" is a correct answer.

CORRECT: "Deploy ElastiCache in each AZ" is also a correct answer.

INCORRECT: "Use an ELB to distribute load between RDS instances" is incorrect. You cannot use an ELB to distributed load between different RDS instances.

INCORRECT: "Migrate to DynamoDB" is incorrect. Moving from a relational DB to a NoSQL DB (DynamoDB) is unlikely to be a viable solution.

INCORRECT: "Use a larger RDS instance size" is incorrect. Using a larger instance size may alleviate the problems the question states that the solution should offload reads from the main DB, read replicas can do this.

References:

<https://aws.amazon.com/rds/features/read-relicas/>

<https://aws.amazon.com/elasticache/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 55

A Solutions Architect is creating a multi-tier application that includes loosely-coupled, distributed application components and needs to determine a method of sending notifications instantaneously. Using Amazon SNS which transport protocols are supported? (Select TWO.)

1. Amazon SWF
2. FTP
3. HTTPS
4. AWS Lambda
5. Email-JSON

Answer: 3,5

Explanation:

Note that the questions asks you which transport protocols are supported, NOT which subscribers – therefore AWS Lambda is not supported.

Amazon SNS supports notifications over multiple transport protocols:

- HTTP/HTTPS – subscribers specify a URL as part of the subscription registration.
- Email/Email-JSON – messages are sent to registered addresses as email (text-based or JSON-object).
- SQS – users can specify an SQS standard queue as the endpoint.
- SMS – messages are sent to registered phone numbers as SMS text messages.

CORRECT: "HTTPS" is the correct answer.

CORRECT: "Email-JSON" is the correct answer.

INCORRECT: "Amazon SWF" is incorrect as this is not a supported transport protocol.

INCORRECT: "FTP" is incorrect as this is not a supported transport protocol.

INCORRECT: "AWS Lambda" is incorrect as this is not a supported transport protocol.

References:

<https://aws.amazon.com/sns/faqs/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/>

QUESTION 56

A manager is concerned that the default service limits may soon be reached for several AWS services. Which AWS tool can a Solutions Architect use to display current usage and limits?

1. AWS Systems Manager
2. AWS Trusted Advisor
3. AWS Dashboard
4. Amazon CloudWatch

Answer: 2

Explanation:

Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.

AWS Trusted Advisor offers a Service Limits check (in the Performance category) that displays your usage and limits for some aspects of some services.

CORRECT: "AWS Trusted Advisor" is the correct answer.

INCORRECT: "AWS Systems Manager" is incorrect. AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources.

INCORRECT: "AWS Dashboard" is incorrect. There is no service known as "AWS Dashboard".

INCORRECT: "Amazon CloudWatch" is incorrect. Amazon CloudWatch is used for performance monitoring not displaying usage limits..

References:

https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

QUESTION 57

A company has multiple AWS accounts for several environments (Prod, Dev, Test etc.). A Solutions Architect would like to copy an Amazon EBS snapshot from DEV to PROD. The snapshot is from an EBS volume that was encrypted with a custom key.

What steps must be performed to share the encrypted EBS snapshot with the Prod account? (Select TWO.)

1. Share the custom key used to encrypt the volume
2. Make a copy of the EBS volume and unencrypt the data in the process
3. Create a snapshot of the unencrypted volume and share it with the Prod account

4. Modify the permissions on the encrypted snapshot to share it with the Prod account
5. Use CloudHSM to distribute the encryption keys used to encrypt the volume

Answer: 1,4

Explanation:

When an EBS volume is encrypted with a custom key you must share the custom key with the PROD account. You also need to modify the permissions on the snapshot to share it with the PROD account. The PROD account must copy the snapshot before they can then create volumes from the snapshot.

Note that you cannot share encrypted volumes created using a default CMK key and you cannot change the CMK key that is used to encrypt a volume.

CORRECT: "Share the custom key used to encrypt the volume" is a correct answer.

CORRECT: "Modify the permissions on the encrypted snapshot to share it with the Prod account" is also a correct answer.

INCORRECT: "Make a copy of the EBS volume and unencrypt the data in the process" is incorrect. You do not need to decrypt the data as there is a workable solution that keeps the data secure at all times.

INCORRECT: "Create a snapshot of the unencrypted volume and share it with the Prod account" is incorrect as the volume is already encrypted as security should be maintained.

INCORRECT: "Use CloudHSM to distribute the encryption keys used to encrypt the volume" is incorrect. CloudHSM is used for key management and storage but not distribution..

References:

<https://aws.amazon.com/blogs/aws/new-cross-account-copying-of-encrypted-ebs-snapshots/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 58

An application you manage runs a number of components using a micro-services architecture. Several ECS container instances in your ECS cluster are displaying as disconnected. The ECS instances were created from the Amazon ECS-Optimized AMI. What steps might you take to troubleshoot the issue? (Select TWO.)

1. Verify that the instances have the correct IAM group applied
2. Verify that the container instances have the container agent installed
3. Verify that the IAM instance profile has the necessary permissions
4. Verify that the container agent is running on the container instances
5. Verify that the container instances are using the Fargate launch type

Answer: 3,4

Explanation:

The ECS container agent is included in the Amazon ECS optimized AMI and can also be installed on any EC2 instance that supports the ECS specification (only supported on EC2 instances). Therefore, you don't need to verify that the agent is installed.

You need to verify that the installed agent is running and that the IAM instance profile has the necessary permissions applied.

Troubleshooting steps for containers include:

- Verify that the Docker daemon is running on the container instance.
- Verify that the Docker Container daemon is running on the container instance.
- Verify that the container agent is running on the container instance.
- Verify that the IAM instance profile has the necessary permissions.

CORRECT: "Verify that the IAM instance profile has the necessary permissions" is the correct answer.

CORRECT: "Verify that the container agent is running on the container instances" is the correct answer.

INCORRECT: "Verify that the instances have the correct IAM group applied" is incorrect. You apply IAM roles (instance profile) to EC2 instances, not groups..

INCORRECT: "Verify that the container instances have the container agent installed" is incorrect as the ECS-optimized AMI has the agent included.

INCORRECT: "Verify that the container instances are using the Fargate launch type" is incorrect. This example is based on the EC2 launch type not the Fargate launch type. With Fargate the infrastructure is managed for you by AWS.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/ecs-agent-disconnected/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/>

QUESTION 59

The application development team in a company have created a new application written in .NET. A Solutions Architect is looking for a way to easily deploy the application whilst maintaining full control of the underlying resources.

Which PaaS service provided by AWS would BEST suit this requirement?

1. CloudFront
2. Elastic Beanstalk
3. EC2 Placement Groups
4. CloudFormation

Answer: 2

Explanation:

AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. It is considered to be a Platform as a Service (PaaS) solution and allows full control of the underlying resources.

CORRECT: "Elastic Beanstalk" is the correct answer.

INCORRECT: "CloudFront" is incorrect. CloudFront is a content delivery network for caching content to improve performance.

INCORRECT: "EC2 Placement Groups" is incorrect. EC2 Placement Groups are used to control how instances are launched to enable low-latency connectivity or to be spread across distinct hardware.

INCORRECT: "CloudFormation" is incorrect. CloudFormation uses templates to provision infrastructure.

References:

<https://aws.amazon.com/elasticbeanstalk/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/>

QUESTION 60

A Solutions Architect is building a small web application running on Amazon EC2 that will be serving static content. The user base is spread out globally and speed is important. Which AWS service can deliver the best user experience cost-effectively and reduce the load on the web server?

1. Amazon RedShift
2. Amazon S3
3. Amazon CloudFront
4. Amazon EBS volume

Answer: 3

Explanation:

This is a good use case for Amazon CloudFront as the user base is spread out globally and CloudFront can cache the content closer to users and also reduce the load on the web server running on EC2.

CORRECT: "Amazon CloudFront" is the correct answer.

INCORRECT: "Amazon RedShift" is incorrect. Amazon RedShift is a data warehouse and is not suitable in this solution.

INCORRECT: "Amazon S3" is incorrect. Amazon S3 is very cost-effective however a bucket is located in a single region and therefore performance is not so great for users a long distance from the bucket.

INCORRECT: "Amazon EBS volume" is incorrect. EBS is not the most cost-effective storage solution and the data would be located in a single region so latency could be an issue.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 61

Amazon CloudWatch is being used to monitor the performance of AWS Lambda. Which metrics does Lambda track? (Select TWO.)

1. Total number of requests
2. Latency per request
3. Number of users
4. Total number of connections
5. Total number of transactions

Answer: 1,2

Explanation:

AWS Lambda automatically monitors Lambda functions and reports metrics through Amazon CloudWatch. Lambda tracks the number of requests, the latency per request, and the number of requests resulting in an error. You can view the request rates and error rates using the AWS Lambda Console, the CloudWatch console, and other AWS resources.

CORRECT: "Total number of requests" is a correct answer.

CORRECT: "Latency per request" is also a correct answer.

INCORRECT: "Number of users" is incorrect as this is not returned.

INCORRECT: "Total number of connections" is incorrect as this is not returned.

INCORRECT: "Total number of transactions" is incorrect as this is not returned.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/monitoring-metrics.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

QUESTION 62

An Amazon EC2 instance running a video on demand web application has been experiencing high CPU utilization. A Solutions Architect needs to take steps to reduce the impact on the EC2 instance and improve performance for consumers. Which of the steps below would help?

1. Use ElastiCache as the web front-end and forward connections to EC2 for cache misses
2. Create a CloudFront distribution and configure a custom origin pointing at the EC2 instance
3. Create an ELB and place it in front of the EC2 instance
4. Create a CloudFront RTMP distribution and point it at the EC2 instance

Answer: 2

Explanation:

This is a good use case for CloudFront which is a content delivery network (CDN) that caches content to improve performance for users who are consuming the content. This will take the load off of the EC2 instances as CloudFront has a cached copy of the video files.

An origin is the origin of the files that the CDN will distribute. Origins can be either an S3 bucket, an EC2 instance, and Elastic Load Balancer, or Route 53 – can also be external (non-AWS).

CORRECT: "Create a CloudFront distribution and configure a custom origin pointing at the EC2 instance" is the correct answer.

INCORRECT: "Use ElastiCache as the web front-end and forward connections to EC2 for cache misses" is incorrect. ElastiCache

cannot be used as an Internet facing web front-end.

INCORRECT: "Create an ELB and place it in front of the EC2 instance" is incorrect. Placing an ELB in front of a single EC2 instance does not help to reduce load.

INCORRECT: "Create a CloudFront RTMP distribution and point it at the EC2 instance" is incorrect. For RTMP CloudFront distributions files must be stored in an S3 bucket.

References:

https://docs.aws.amazon.com/cloudfront/latest/APIReference/API_Origin.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 63

A Solutions Architect needs to create a file system that can be concurrently accessed by multiple Amazon EC2 instances across multiple availability zones. The file system needs to support high throughput and the ability to burst. As the data that will be stored on the file system will be sensitive, it must be encrypted at rest and in transit.

Which storage solution should the Solutions Architect use for the shared file system?

1. Add EBS volumes to each EC2 instance and configure data replication
2. Use the Elastic Block Store (EBS) and mount the file system at the block level
3. Use the Elastic File System (EFS) and mount the file system using NFS
4. Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

Answer: 3

Explanation:

EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. EFS file systems are mounted using the NFSv4.1 protocol. EFS is designed to burst to allow high throughput levels for periods of time. EFS also offers the ability to encrypt data at rest and in transit.

CORRECT: "Use the Elastic File System (EFS) and mount the file system using NFS" is the correct answer.

INCORRECT: "Add EBS volumes to each EC2 instance and configure data replication" is incorrect. Adding EBS volumes to each instance and configuring data replication is not the best solution for this scenario and there is no native capability within AWS for performing the replication. Some 3rd party data management software does use this model, however.

INCORRECT: "Use the Elastic Block Store (EBS) and mount the file system at the block level" is incorrect. EBS is a block-level storage system not a file-level storage system. You cannot mount EBS volumes from multiple instances across AZs.

INCORRECT: "Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes" is incorrect. You cannot use an ELB to distribute data between EBS volumes.

References:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 64

A new department will begin using AWS services an AWS account and a Solutions Architect needs to create an authentication and authorization strategy. Select the correct statements regarding IAM groups? (Select TWO.)

1. IAM groups can be used to assign permissions to users
2. IAM groups can be nested up to 4 levels
3. IAM groups can be used to group EC2 instances
4. IAM groups can temporarily assume a role to take on permissions for a specific task
5. An IAM group is not an identity and cannot be identified as a principal in an IAM policy

Answer: 1,5

Explanation:

An IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

The following facts apply to IAM Groups:

- Groups are collections of users and have policies attached to them.
- A group is not an identity and cannot be identified as a principal in an IAM policy.
- Use groups to assign permissions to users.
- IAM groups cannot be used to group EC2 instances.
- Only users and services can assume a role to take on permissions (not groups).

CORRECT: "IAM groups can be used to assign permissions to users" is a correct answer.

CORRECT: "An IAM group is not an identity and cannot be identified as a principal in an IAM policy" is also a correct answer.

INCORRECT: "IAM groups can be nested up to 4 levels" is incorrect as this is not possible.

INCORRECT: "IAM groups can be used to group EC2 instances" is incorrect as they can only be used to group user accounts.

INCORRECT: "IAM groups can temporarily assume a role to take on permissions for a specific task" is incorrect as this is not possible.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 65

The development team in a media organization is moving their SDLC processes into the AWS Cloud. Which AWS service can a Solutions Architect recommend that is primarily used for software version control?

1. CloudHSM
2. CodeStar
3. CodeCommit
4. Step Functions

Answer: 3

Explanation:

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.

CORRECT: "CodeCommit" is the correct answer.

INCORRECT: "CloudHSM" is incorrect. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud

INCORRECT: "CodeStar" is incorrect. AWS CodeStar enables you to quickly develop, build, and deploy applications on AWS..

INCORRECT: "Step Functions" is incorrect. AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly.

References:

<https://aws.amazon.com/codecommit/>

SET 6: PRACTICE QUESTIONS ONLY

For training purposes, go directly to [Set 6: Practice Questions, Answers & Explanations](#)

QUESTION 1

A company runs a streaming media service and the content is stored on Amazon S3. The media catalog server pulls updated content from S3 and can issue over 1 million read operations per second for short periods. Latency must be kept under 5ms for these updates. Which solution will provide the BEST performance for the media catalog updates?

1. Update the application code to use an Amazon ElastiCache for Redis cluster
2. Implement Amazon CloudFront and cache the content at Edge Locations
3. Update the application code to use an Amazon DynamoDB Accelerator cluster
4. Implement an Instance store volume on the media catalog server

QUESTION 2

Three AWS accounts are owned by the same company but in different regions. Account Z has two AWS Direct Connect connections to two separate company offices. Accounts A and B require the ability to route across account Z's Direct Connect connections to each company office. A Solutions Architect has created an AWS Direct Connect gateway in account Z.

How can the required connectivity be configured?

1. Associate the Direct Connect gateway to a transit gateway in each region
2. Associate the Direct Connect gateway to a virtual private gateway in account A and B
3. Create a VPC Endpoint to the Direct Connect gateway in account A and B
4. Create a PrivateLink connection in Account Z and ENIs in accounts A and B

QUESTION 3

A tool needs to analyze data stored in an Amazon S3 bucket. Processing the data takes a few seconds and results are then written to another S3 bucket. Less than 256 MB of memory is needed to run the process. What would be the MOST cost-effective compute solutions for this use case?

1. AWS Fargate tasks
2. AWS Lambda functions
3. Amazon EC2 spot instances
4. Amazon Elastic Beanstalk

QUESTION 4

An application makes calls to a REST API running on Amazon EC2 instances behind an Application Load Balancer (ALB). Most API calls complete quickly. However, a single endpoint is making API calls that require much longer to complete and this is introducing overall latency into the system. What steps can a Solutions Architect take to minimize the effects of the long-running API calls?

1. Change the EC2 instance to one with enhanced networking to reduce latency
2. Create an Amazon SQS queue and decouple the long-running API calls
3. Increase the ALB idle timeout to allow the long-running requests to complete
4. Change the ALB to a Network Load Balancer (NLB) and use SSL/TLS termination

QUESTION 5

An application runs on EC2 instances in a private subnet behind an Application Load Balancer in a public subnet. The application is highly available and distributed across multiple AZs. The EC2 instances must make API calls to an internet-based service. How can the Solutions Architect enable highly available internet connectivity?

1. Create a NAT gateway and attach it to the VPC. Add a route to the gateway to each private subnet route table
2. Configure an internet gateway. Add a route to the gateway to each private subnet route table

3. Create a NAT instance in the private subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT instance
4. Create a NAT gateway in the public subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT gateway

QUESTION 6

A legacy application is being migrated into AWS. The application has a large amount of data that is rarely accessed. When files are accessed they are retrieved sequentially. The application will be migrated onto an Amazon EC2 instance.

What is the LEAST expensive EBS volume type for this use case?

1. Cold HDD (sc1)
2. Provisioned IOPS SSD (io1)
3. General Purpose SSD (gp2)
4. Throughput Optimized HDD (st1)

QUESTION 7

An application uses an Amazon RDS database and Amazon EC2 instances in a web tier. The web tier instances must not be directly accessible from the internet to improve security.

How can a Solutions Architect meet these requirements?

1. Launch the EC2 instances in a private subnet and create an Application Load Balancer in a public subnet
2. Launch the EC2 instances in a private subnet with a NAT gateway and update the route table
3. Launch the EC2 instances in a public subnet and use AWS WAF to protect the instances from internet-based attacks
4. Launch the EC2 instances in a public subnet and create an Application Load Balancer in a public subnet

QUESTION 8

A company runs an application on premises that stores a large quantity of semi-structured data using key-value pairs. The application code will be migrated to AWS Lambda and a highly scalable solution is required for storing the data.

Which datastore will be the best fit for these requirements?

1. Amazon EFS
2. Amazon RDS MySQL
3. Amazon EBS
4. Amazon DynamoDB

QUESTION 9

An application uses a MySQL database running on an Amazon EC2 instance. The application generates high I/O and constant writes to a single table on the database. Which Amazon EBS volume type will provide the MOST consistent performance and low latency?

1. General Purpose SSD (gp2)
2. Provisioned IOPS SSD (io1)
3. Throughput Optimized HDD (st1)
4. Cold HDD (sc1)

QUESTION 10

A Solutions Architect needs to capture information about the traffic that reaches an Amazon Elastic Load Balancer. The information should include the source, destination, and protocol.

What is the most secure and reliable method for gathering this data?

1. Create a VPC flow log for each network interface associated with the ELB
2. Enable Amazon CloudTrail logging and configure packet capturing
3. Use Amazon CloudWatch Logs to review detailed logging information
4. Create a VPC flow log for the subnets in which the ELB is running

QUESTION 11

The Solutions Architect in charge of a critical application must ensure the Amazon EC2 instances are able to be launched in another AWS Region in the event of a disaster.

What steps should the Solutions Architect take? (Select TWO.)

1. Launch instances in the second Region using the S3 API
2. Create AMIs of the instances and copy them to another Region
3. Enable cross-region snapshots for the Amazon EC2 instances
4. Launch instances in the second Region from the AMIs
5. Copy the snapshots using Amazon S3 cross-region replication

QUESTION 12

A company needs to ensure that they can failover between AWS Regions in the event of a disaster seamlessly with minimal downtime and data loss. The applications will run in an active-active configuration.

Which DR strategy should a Solutions Architect recommend?

1. Backup and restore
2. Pilot light
3. Warm standby
4. Multi-site

QUESTION 13

A company has launched a multi-tier application architecture. The web tier and database tier run on Amazon EC2 instances in private subnets within the same Availability Zone.

Which combination of steps should a Solutions Architect take to add high availability to this architecture? (Select TWO.)

1. Create new public subnets in the same AZ for high availability and move the web tier to the public subnets
2. Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs
3. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)
4. Create new private subnets in the same VPC but in a different AZ. Create a database using Amazon EC2 in one AZ
5. Create new private subnets in the same VPC but in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment

QUESTION 14

An on-premises server runs a MySQL database and will be migrated to the AWS Cloud. The company require a managed solution that supports high availability and automatic failover in the event of the outage of an Availability Zone (AZ).

Which solution is the BEST fit for these requirements?

1. Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon RDS MySQL Multi-AZ deployment
2. Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon EC2 MySQL Multi-AZ deployment
3. Create a snapshot of the MySQL database server and use AWS DataSync to migrate the data Amazon S3. Launch a new Amazon RDS MySQL Multi-AZ deployment from the snapshot
4. Use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon RDS MySQL. Use the Schema Conversion Tool (SCT) to enable conversion from MySQL to Amazon RDS

QUESTION 15

The database layer of an on-premises web application is being migrated to AWS. The database currently uses an in-memory cache. A Solutions Architect must deliver a solution that supports high availability and replication for the caching layer.

Which service should the Solutions Architect recommend?

1. Amazon ElastiCache Redis
2. Amazon RDS Multi-AZ
3. Amazon ElastiCache Memcached

4. Amazon DynamoDB

QUESTION 16

A Solutions Architect has created an AWS Organization with several AWS accounts. Security policy requires that use of specific API actions are limited across all accounts. The Solutions Architect requires a method of centrally controlling these actions.

What is the SIMPLEST method of achieving the requirements?

1. Create a Network ACL that limits access to the services or actions and attach it to all relevant subnets
2. Create an IAM policy in the root account and attach it to users and groups in each account
3. Create cross-account roles in each account to limit access to the services and actions that are allowed
4. Create a service control policy in the root organizational unit to deny access to the services or actions

QUESTION 17

A company has a fleet of Amazon EC2 instances behind an Elastic Load Balancer (ELB) that are a mixture of c4.2xlarge instance types and c5.large instances. The load on the CPUs on the c5.large instances has been very high, often hitting 100% utilization, whereas the c4.2xlarge instances have been performing well.

What should a Solutions Architect recommend to resolve the performance issues?

1. Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances
2. Add all of the instances into a Placement Group
3. Change the configuration to use only c4.2xlarge instance types
4. Add more c5.large instances to spread the load more evenly

QUESTION 18

A Solutions Architect created a new IAM user account for a temporary employee who recently joined the company. The user does not have permissions to perform any actions, which statement is true about newly created users in IAM?

1. They are created with no permissions
2. They are created with limited permissions
3. They are created with full permissions
4. They are created with user privileges

QUESTION 19

A government agency is using CloudFront for a web application that receives personally identifiable information (PII) from citizens. What feature of CloudFront applies an extra level of encryption at CloudFront edge locations to ensure the PII data is secured end-to-end?

1. Object invalidation
2. Field-level encryption
3. RTMP distribution
4. Origin access identity

QUESTION 20

A company has multiple Amazon VPCs that are peered with each other. The company would like to use a single Elastic Load Balancer (ELB) to route traffic to multiple EC2 instances in peered VPCs within the same region. How can this be achieved?

1. This is not possible, the instances that an ELB routes traffic to must be in the same VPC
2. This is possible using the Classic Load Balancer (CLB) if using Instance IDs
3. This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets
4. This is not possible with ELB, you would need to use Route 53

QUESTION 21

Some data has become corrupted in an Amazon RDS database. A Solutions Architect plans to use point-in-time restore to recover the data to the last known good configuration. Which of the following statements is correct about restoring an RDS database to a specific point-in-time? (Select TWO.)

1. You can restore up to the last 5 minutes
2. Custom DB security groups are applied to the new DB instance
3. You can restore up to the last 1 minute
4. The default DB security group is applied to the new DB instance
5. The database restore overwrites the existing database

QUESTION 22

An application is generating a large amount of clickstream events data that is being stored on S3. The business needs to understand customer behavior and want to run complex analytics queries against the data.

Which AWS service can be used for this requirement?

1. Amazon RedShift
2. Amazon Neptune
3. Amazon RDS
4. Amazon Kinesis Firehose

QUESTION 23

A Solutions Architect is deploying a production application that will use several Amazon EC2 instances and run constantly on an ongoing basis. The application cannot be interrupted or restarted. Which EC2 pricing model would be best for this workload?

1. Reserved instances
2. On-demand instances
3. Spot instances
4. Flexible instances

QUESTION 24

A customer has requested some advice on how to implement security measures in their Amazon VPC. The client has recently been the victim of some hacking attempts. The client wants to implement measures to mitigate further threats. The client has explained that the attacks always come from the same small block of IP addresses.

What would be a quick and easy measure to help prevent further attacks?

1. Use a Security Group rule that denies connections from the block of IP addresses
2. Use CloudFront's DDoS prevention features
3. Create a Bastion Host restrict all connections to the Bastion Host only
4. Use a Network ACL rule that denies connections from the block of IP addresses

QUESTION 25

An Amazon EC2 instance has been launched into an Amazon VPC. A Solutions Architect needs to ensure that instances have both a private and public DNS hostnames. Assuming settings were not changed during creation of the VPC, how will DNS hostnames be assigned by default? (Select TWO.)

1. In all VPCs instances no DNS hostnames will be assigned
2. In a non-default VPC instances will be assigned a public and private DNS hostname
3. In a default VPC instances will be assigned a public and private DNS hostname
4. In a non-default VPC instances will be assigned a private but not a public DNS hostname
5. In a default VPC instances will be assigned a private but not a public DNS hostname

QUESTION 26

A fleet of Amazon EC2 instances running Linux will be launched in an Amazon VPC. An application development framework and some custom software must be installed on the instances. The installation will be initiated using some scripts. What feature enables a Solutions Architect to specify the scripts the software can be installed during the EC2 instance launch?

1. Metadata
2. Run Command
3. AWS Config
4. User Data

QUESTION 27

A company is investigating ways to analyze and process large amounts of data in the cloud faster, without needing to load or transform the data in a data warehouse. The data resides in Amazon S3.

Which AWS services would allow the company to query the data in place? (Select TWO.)

1. Amazon S3 Select
2. Amazon Kinesis Data Streams
3. Amazon Elasticsearch
4. Amazon RedShift Spectrum
5. Amazon SWF

QUESTION 28

A distribution method is required for some static files. The requests will mainly be GET requests and a high volume of GETs is expected, often exceeding 2000 per second. The files are currently stored in an S3 bucket. According to AWS best practices, how can performance be optimized?

1. Use cross-region replication to spread the load across regions
2. Use ElastiCache to cache the content
3. Integrate CloudFront with S3 to cache the content
4. Use S3 Transfer Acceleration

QUESTION 29

An Auto Scaling group of Amazon EC2 instances behind an Elastic Load Balancer (ELB) is running in an Amazon VPC. Health checks are configured on the ASG to use EC2 status checks. The ELB has determined that an EC2 instance is unhealthy and has removed it from service. A Solutions Architect noticed that the instance is still running and has not been terminated by EC2 Auto Scaling.

What would be an explanation for this behavior?

1. The ASG is waiting for the cooldown timer to expire before terminating the instance
2. Connection draining is enabled and the ASG is waiting for in-flight requests to complete
3. The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service
4. The health check grace period has not yet expired

QUESTION 30

A financial services company regularly runs an analysis of the day's transaction costs, execution reporting, and market performance. The company currently uses third-party commercial software for provisioning, managing, monitoring, and scaling the computing jobs which utilize a large fleet of EC2 instances.

The company is seeking to reduce costs and utilize AWS services. Which AWS service could be used in place of the third-party software?

1. Amazon Athena
2. AWS Systems Manager
3. Amazon Lex
4. AWS Batch

QUESTION 31

A customer is deploying services in a hybrid cloud model. The customer has mandated that data is transferred directly between cloud data centers, bypassing ISPs.

Which AWS service can be used to enable hybrid cloud connectivity?

1. AWS Direct Connect
2. Amazon VPC
3. IPSec VPN
4. Amazon Route 53

QUESTION 32

An Amazon Elastic File System (EFS) has been created to store data that will be accessed by a large number of Amazon EC2 instances. The data is sensitive and a Solutions Architect is creating a design for security measures to protect the data. It is required that network traffic is restricted correctly based on firewall rules and access from hosts is restricted by user or group.

How can this be achieved with Amazon EFS? (Select TWO.)

1. Use POSIX permissions to control access from hosts by user or group
2. Use AWS Web Application Firewall (WAF) to protect EFS
3. Use EFS Security Groups to control network traffic
4. Use Network ACLs to control the traffic
5. Use IAM groups to control access by user or group

QUESTION 33

A large multi-national client has requested a design for a multi-region database. The master database will be in the EU (Frankfurt) region and databases will be located in 4 other regions to service local read traffic. The database should be a managed service including the replication.

The solution should be cost-effective and secure. Which AWS service can deliver these requirements?

1. RDS with Multi-AZ
2. EC2 instances with EBS replication
3. RDS with cross-region Read Replicas
4. ElastiCache with Redis and clustering mode enabled

QUESTION 34

A Solutions Architect is designing the system monitoring and deployment layers of a serverless application. The system monitoring layer will manage system visibility through recording logs and metrics and the deployment layer will deploy the application stack and manage workload changes through a release management process.

The Architect needs to select the most appropriate AWS services for these functions. Which services and frameworks should be used for the system monitoring and deployment layers? (Select TWO.)

1. Use AWS CloudTrail for consolidating system and application logs and monitoring custom metrics
2. Use AWS X-Ray to package, test, and deploy the serverless application stack
3. Use AWS SAM to package, test, and deploy the serverless application stack
4. Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics
5. Use AWS Lambda to package, test, and deploy the serverless application stack

QUESTION 35

One of the departments in a company has been generating a large amount of data on Amazon S3 and costs are increasing. Data older than 90 days is rarely accessed but must be retained for several years. If this data does need to be accessed at least 24 hours notice is provided.

How can a Solutions Architect optimize the costs associated with storage of this data whilst ensuring it is accessible if required?

1. Implement archival software that automatically moves the data to tape
2. Use S3 lifecycle policies to move data to the STANDARD_IA storage class
3. Use S3 lifecycle policies to move data to GLACIER after 90 days
4. Select the older data and manually migrate it to GLACIER

QUESTION 36

A Solutions Architect enabled Access Logs on an Application Load Balancer (ALB) and needs to process the log files using a hosted Hadoop service. What configuration changes and services can be leveraged to deliver this requirement?

1. Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files
2. Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files
3. Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files
4. Configure Access Logs to be delivered to S3 and use EMR for processing the log files

QUESTION 37

A web application receives order processing information from customers and places the messages on an Amazon SQS queue. A fleet of Amazon EC2 instances are configured to pick up the messages, process them, and store the results in a DynamoDB table. The current configuration has been resulting in a large number of empty responses to **ReceiveMessage** API requests.

A Solutions Architect needs to eliminate empty responses to reduce operational overhead. How can this be done?

1. Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once
2. Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received
3. Configure Long Polling to eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response
4. Configure Short Polling to eliminate empty responses by reducing the length of time a connection request remains open

QUESTION 38

A Solutions Architect has created an AWS account and selected the Asia Pacific (Sydney) region. Within the default VPC there is a default security group. What settings are configured within this security group by default? (Select TWO.)

1. There is an inbound rule that allows all traffic from the security group itself
2. There is an inbound rule that allows all traffic from any address
3. There is an outbound rule that allows all traffic to the security group itself
4. There is an outbound rule that allows all traffic to all addresses
5. There is an outbound rule that allows traffic to the VPC router

QUESTION 39

A company is deploying a new two-tier web application that uses EC2 web servers and a DynamoDB database backend. An Internet facing ELB distributes connections between the web servers.

The Solutions Architect has created a security group for the web servers and needs to create a security group for the ELB. What rules should be added? (Select TWO.)

1. Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group
2. Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway
3. Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR
4. Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0
5. Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32

QUESTION 40

A development team needs to run up a few lab servers on a weekend for a new project. The servers will need to run uninterrupted for a few hours. Which EC2 pricing option would be most suitable?

1. Spot
2. Reserved
3. On-Demand
4. Dedicated Instances

QUESTION 41

A Solutions Architect has logged into an Amazon EC2 Linux instance using SSH and needs to determine a few pieces of information including what IAM role is assigned, the instance ID and the names of the security groups that are assigned to the instance.

From the options below, what would be the best source of this information?

1. Metadata
2. Tags
3. User data
4. Parameters

QUESTION 42

An Amazon EC2 instance is generating very high packets-per-second and performance of the application stack is being impacted. A Solutions Architect needs to determine a resolution to the issue that results in improved performance.

Which action should the Architect take?

1. Configure a RAID 1 array from multiple EBS volumes
2. Create a placement group and put the EC2 instance in it
3. Use enhanced networking
4. Add multiple Elastic IP addresses to the instance

QUESTION 43

A company runs a web-based application that uses Amazon EC2 instances for the web front-end and Amazon RDS for the database back-end. The web application writes transaction log files to an Amazon S3 bucket and the quantity of files is becoming quite large. It is acceptable to retain the most recent 60 days of log files and permanently delete the rest.

Which action can a Solutions Architect take to enable this to happen automatically?

1. Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old
2. Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old
3. Use an S3 bucket policy that deletes objects that are more than 60 days old
4. Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class

QUESTION 44

A Solutions Architect needs to upload a large (2GB) file to an S3 bucket. What is the recommended way to upload a single large file to an S3 bucket?

1. Use AWS Import/Export
2. Use Multipart Upload
3. Use a single PUT request to upload the large file
4. Use Amazon Snowball

QUESTION 45

Several Amazon EC2 Spot instances are being used to process messages from an Amazon SQS queue and store results in an Amazon DynamoDB table. Shortly after picking up a message from the queue AWS terminated the Spot instance. The Spot instance had not finished processing the message. What will happen to the message?

1. The message will become available for processing again after the visibility timeout expires
2. The message will be lost as it would have been deleted from the queue when processed
3. The message will remain in the queue and be immediately picked up by another instance
4. The results may be duplicated in DynamoDB as the message will likely be processed multiple times

QUESTION 46

A company is transitioning their web presence into the AWS cloud. As part of the migration the company will be running a web application both on-premises and in AWS for a period of time. During the period of co-existence the client would like 80% of the traffic to hit the AWS-based web servers and 20% to be directed to the on-premises web servers.

What method can a Solutions Architect use to distribute traffic as requested?

1. Use Route 53 with a weighted routing policy and configure the respective weights
2. Use Route 53 with a simple routing policy
3. Use an Application Load Balancer to distribute traffic based on IP address
4. Use a Network Load Balancer to distribute traffic based on Instance ID

QUESTION 47

A Solutions Architect has created a new Network ACL in an Amazon VPC. No rules have been created. Which of the statements below are correct regarding the default state of the Network ACL? (Select TWO.)

1. There is a default inbound rule allowing traffic from the VPC CIDR block
2. There is a default outbound rule allowing traffic to the Internet Gateway
3. There is a default outbound rule allowing all traffic
4. There is a default inbound rule denying all traffic
5. There is a default outbound rule denying all traffic

QUESTION 48

A company needs to capture detailed information about all HTTP requests that are processed by their Internet facing Application Load Balancer (ALB). The company requires information on the requester, IP address, and request type for analyzing traffic patterns to better understand their customer base.

Which actions should a Solutions Architect recommend?

1. Configure metrics in CloudWatch for the ALB
2. Enable EC2 detailed monitoring
3. Enable Access Logs and store the data on S3
4. Use CloudTrail to capture all API calls made to the ALB

QUESTION 49

A Solutions Architect needs to run a PowerShell script on a fleet of Amazon EC2 instances running Microsoft Windows. The instances have already been launched in an Amazon VPC. What tool can be run from the AWS Management Console that to execute the script on all target EC2 instances?

1. AWS CodeDeploy
2. AWS Config
3. Run Command
4. AWS OpsWorks

QUESTION 50

A company requires an Elastic Load Balancer (ELB) for an application they are planning to deploy on AWS. The application requires extremely high throughput and extremely low latencies. The connections will be made using the TCP protocol and the ELB must support load balancing to multiple ports on an instance. Which ELB would should the company use?

1. Classic Load Balancer
2. Application Load Balancer
3. Network Load Balancer
4. Route 53

QUESTION 51

A web application runs on a series of Amazon EC2 instances behind an Application Load Balancer (ALB). A Solutions Architect is updating the configuration with a health check and needs to select the protocol to use. What options are available? (Select TWO.)

1. HTTP
2. SSL
3. **HTTPS**
4. TCP
5. ICMP

QUESTION 52

A Solutions Architect is designing the disk configuration for an Amazon EC2 instance. The instance needs to support a MapReduce process that requires high throughput for a large dataset with large I/O sizes.

Which Amazon EBS volume is the MOST cost-effective solution for these requirements?

1. EBS General Purpose SSD in a RAID 1 configuration
2. EBS Throughput Optimized HDD
3. EBS Provisioned IOPS SSD

4. EBS General Purpose SSD

QUESTION 53

An Amazon EBS-backed EC2 instance has been launched. A requirement has come up for some high-performance ephemeral storage.

How can a Solutions Architect add a new instance store volume?

1. You must shutdown the instance in order to be able to add the instance store volume
2. You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume
3. You can specify the instance store volumes for your instance only when you launch an instance
4. You can use a block device mapping to specify additional instance store volumes when you launch your instance, or you can attach additional instance store volumes after your instance is running

QUESTION 54

A large quantity of data that is rarely accessed is being archived onto Amazon Glacier. Your CIO wants to understand the resilience of the service. Which of the statements below is correct about Amazon Glacier storage? (Select TWO.)

1. Data is replicated globally
2. Provides 99.999999999% durability of archives
3. Data is resilient in the event of one entire Availability Zone destruction
4. Data is resilient in the event of one entire region destruction
5. Provides 99.9% availability of archives

QUESTION 55

A Solutions Architect is launching an Amazon EC2 instance with multiple attached volumes by modifying the block device mapping. Which block device can be specified in a block device mapping to be used with an EC2 instance? (Select TWO.)

1. EBS volume
2. EFS volume
3. Instance store volume
4. Snapshot
5. S3 bucket

QUESTION 56

An Amazon EC2 instance behind an Elastic Load Balancer (ELB) is in the process of being de-registered. Which ELB feature is used to allow existing connections to close cleanly?

1. Sticky Sessions
2. Proxy Protocol
3. Deletion Protection
4. Connection Draining

QUESTION 57

The load on a MySQL database running on Amazon EC2 is increasing and performance has been impacted. Which of the options below would help to increase storage performance? (Select TWO.)

1. Use a larger instance size within the instance family
2. Use HDD, Cold (SC1) EBS volumes
3. Use Provisioned IOPS (IO1) EBS volumes
4. Use EBS optimized instances
5. Create a RAID 1 array from multiple EBS volumes

QUESTION 58

An application receives a high traffic load between 7:30am and 9:30am daily. The application uses an Auto Scaling group to maintain three instances most of the time but during the peak period it requires six instances.

How can a Solutions Architect configure Auto Scaling to perform a daily scale-out event at 7:30am and a scale-in event at 9:30am to account for the peak load?

1. Use a Simple scaling policy
2. Use a Scheduled scaling policy
3. Use a Dynamic scaling policy
4. Use a Step scaling policy

QUESTION 59

An on-premise data center will be connected to an Amazon VPC by a hardware VPN that has public and VPN-only subnets. The security team has requested that traffic hitting public subnets on AWS that's destined to on-premise applications must be directed over the VPN to the corporate firewall.

How can this be achieved?

1. In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway
2. In the public subnet route table, add a route for your remote network and specify the customer gateway as the target
3. Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway
4. In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target

QUESTION 60

An Amazon DynamoDB table has a variable load, ranging from sustained heavy usage some days, to only having small spikes on others. The load is 80% read and 20% write. The provisioned throughput capacity has been configured to account for the heavy load to ensure throttling does not occur.

What would be the most efficient solution to optimize cost?

1. Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput
2. Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput
3. Use DynamoDB DAX to increase the performance of the database
4. Create a DynamoDB Auto Scaling scaling policy

QUESTION 61

A Solutions Architect has created a VPC and is in the process of formulating the subnet design. The VPC will be used to host a two-tier application that will include Internet facing web servers, and internal-only DB servers. Zonal redundancy is required.

How many subnets are required to support this requirement?

1. 2 subnets
2. 6 subnets
3. 1 subnet
4. 4 subnets

QUESTION 62

The application development team in a company have developed a Java application and saved the source code in a .war file. They would like to run the application on AWS resources and are looking for a service that can handle the provisioning and management of the underlying resources it will run on.

Which AWS service should a Solutions Architect recommend the Developers use to upload the Java source code file?

1. AWS Elastic Beanstalk
2. AWS CodeDeploy
3. AWS CloudFormation
4. AWS OpsWorks

QUESTION 63

A Solutions Architect has created a new security group in an Amazon VPC. No rules have been created. Which of the statements

below are correct regarding the default state of the security group? (Select TWO.)

1. There is an outbound rule that allows all traffic to all IP addresses
2. There are no inbound rules and traffic will be implicitly denied
3. There is an inbound rule allowing traffic from the Internet to port 22 for management
4. There are is an inbound rule that allows traffic from the Internet Gateway
5. There is an outbound rule allowing traffic to the Internet Gateway

QUESTION 64

A security officer has requested that all data associated with a specific customer is encrypted. The data resides on Elastic Block Store (EBS) volumes. Which of the following statements about using EBS encryption are correct? (Select TWO.)

1. Not all EBS types support encryption
2. All attached EBS volumes must share the same encryption state
3. All instance types support encryption
4. Data in transit between an instance and an encrypted volume is also encrypted
5. There is no direct way to change the encryption state of a volume

QUESTION 65

An organization in the agriculture sector is deploying sensors and smart devices around factory plants and fields. The devices will collect information and send it to cloud applications running on AWS.

Which AWS service will securely connect the devices to the cloud applications?

1. AWS Glue
2. AWS IoT Core
3. AWS DMS
4. AWS Lambda

SET 6: PRACTICE QUESTIONS AND ANSWERS

QUESTION 1

A company runs a streaming media service and the content is stored on Amazon S3. The media catalog server pulls updated content from S3 and can issue over 1 million read operations per second for short periods. Latency must be kept under 5ms for these updates. Which solution will provide the BEST performance for the media catalog updates?

1. Update the application s volume on the media catalog server
2. Implement Amazon CloudFront and cache the content at Edge Locations
3. Update the application code to use an Amazon DynamoDB Accelerator cluster
4. Implement an Instance store volume on the media catalog server

Answer: 1

Explanation:

Some applications, such as media catalog updates require high frequency reads, and consistent throughput. For such applications, customers often complement S3 with an in-memory cache, such as Amazon ElastiCache for Redis, to reduce the S3 retrieval cost and to improve performance.

ElastiCache for Redis is a fully managed, in-memory data store that provides sub-millisecond latency performance with high throughput. ElastiCache for Redis complements S3 in the following ways:

- Redis stores data in-memory, so it provides sub-millisecond latency and supports incredibly high requests per second.
- It supports key/value based operations that map well to S3 operations (for example, GET/SET => GET/PUT), making it easy to write code for both S3 and ElastiCache.
- It can be implemented as an application side cache. This allows you to use S3 as your persistent store and benefit from its durability, availability, and low cost. Your applications decide what objects to cache, when to cache them, and how to cache them.

In this example the media catalog is pulling updates from S3 so the performance between these components is what needs to be improved. Therefore, using ElastiCache to cache the content will dramatically increase the performance.

CORRECT: "Update the application code to use an Amazon ElastiCache for Redis cluster" is the correct answer.

INCORRECT: "Implement Amazon CloudFront and cache the content at Edge Locations" is incorrect. CloudFront is good for getting media closer to users but in this case we're trying to improve performance within the data center moving data from S3 to the media catalog server.

INCORRECT: "Update the application code to use an Amazon DynamoDB Accelerator cluster" is incorrect. DynamoDB Accelerator (DAX) is used with DynamoDB but is unsuitable for use with Amazon S3.

INCORRECT: "Implement an Instance store volume on the media catalog server" is incorrect. This will improve local disk performance but will not improve reads from Amazon S3.

References:

<https://aws.amazon.com/blogs/storage/turbocharge-amazon-s3-with-amazon-elasticsearch-for-redis/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticsearch/>

QUESTION 2

Three AWS accounts are owned by the same company but in different regions. Account Z has two AWS Direct Connect connections to two separate company offices. Accounts A and B require the ability to route across account Z's Direct Connect connections to each company office. A Solutions Architect has created an AWS Direct Connect gateway in account Z.

How can the required connectivity be configured?

1. Associate the Direct Connect gateway to a transit gateway in each region
2. Associate the Direct Connect gateway to a virtual private gateway in account A and B
3. Create a VPC Endpoint to the Direct Connect gateway in account A and B
4. Create a PrivateLink connection in Account Z and ENIs in accounts A and B

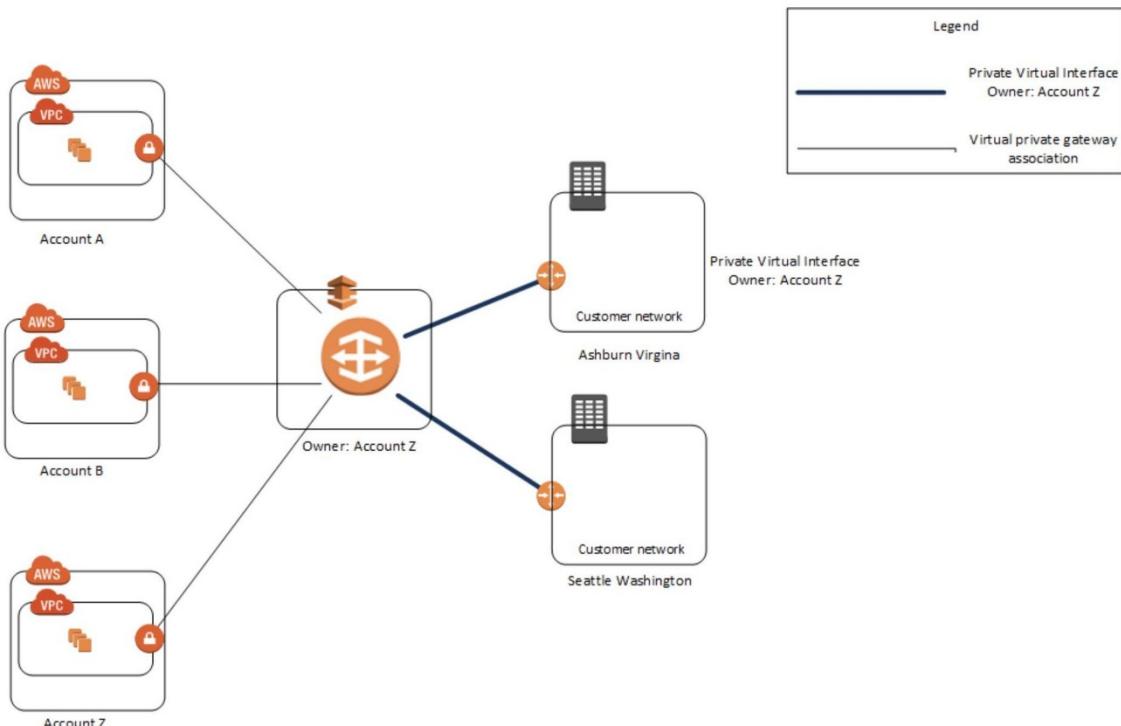
Answer: 2

Explanation:

You can associate an AWS Direct Connect gateway with either of the following gateways:

- A transit gateway when you have multiple VPCs in the same Region.
- A virtual private gateway.

In this case account Z owns the Direct Connect gateway so a VPG in accounts A and B must be associated with it to enable this configuration to work. After Account Z accepts the proposals, Account A and Account B can route traffic from their virtual private gateway to the Direct Connect gateway.



CORRECT: "Associate the Direct Connect gateway to a virtual private gateway in account A and B" is the correct answer.

INCORRECT: "Associate the Direct Connect gateway to a transit gateway in each region" is incorrect. This would be a good solution if the accounts were in VPCs within a region rather than across regions.

INCORRECT: "Create a VPC Endpoint to the Direct Connect gateway in account A and B" is incorrect. You cannot create a VPC endpoint for Direct Connect gateways.

INCORRECT: "Create a PrivateLink connection in Account Z and ENIs in accounts A and B" is incorrect. You cannot use PrivateLink connections to publish a Direct Connect gateway.

References:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

QUESTION 3

A tool needs to analyze data stored in an Amazon S3 bucket. Processing the data takes a few seconds and results are then written to another S3 bucket. Less than 256 MB of memory is needed to run the process. What would be the MOST cost-effective compute solutions for this use case?

1. AWS Fargate tasks
2. AWS Lambda functions
3. Amazon EC2 spot instances
4. Amazon Elastic Beanstalk

Answer: 2

Explanation:

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Lambda has a maximum execution time of 900 seconds and memory can be allocated up to 3008 MB. Therefore, the most cost-effective solution will be AWS Lambda.

CORRECT: "AWS Lambda functions" is the correct answer.

INCORRECT: "AWS Fargate tasks" is incorrect. Fargate runs Docker containers and is serverless. However, you do pay for the running time of the tasks so it will not be as cost-effective.

INCORRECT: "Amazon EC2 spot instances" is incorrect. EC2 instances must run continually waiting for jobs to process so even with spot this would be less cost-effective (and subject to termination).

INCORRECT: "Amazon Elastic Beanstalk" is incorrect. This service also relies on Amazon EC2 instances so would not be as cost-effective.

References:

<https://aws.amazon.com/lambda/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

QUESTION 4

An application makes calls to a REST API running on Amazon EC2 instances behind an Application Load Balancer (ALB). Most API calls complete quickly. However, a single endpoint is making API calls that require much longer to complete and this is introducing overall latency into the system. What steps can a Solutions Architect take to minimize the effects of the long-running API calls?

1. Change the EC2 instance to one with enhanced networking to reduce latency
2. Create an Amazon SQS queue and decouple the long-running API calls
3. Increase the ALB idle timeout to allow the long-running requests to complete
4. Change the ALB to a Network Load Balancer (NLB) and use SSL/TLS termination

Answer: 2

Explanation:

An Amazon Simple Queue Service (SQS) can be used to offload and decouple the long-running requests. They can then be processed asynchronously by separate EC2 instances. This is the best way to reduce the overall latency introduced by the long-running API call.

CORRECT: "Create an Amazon SQS queue and decouple the long-running API calls" is the correct answer.

INCORRECT: "Change the EC2 instance to one with enhanced networking to reduce latency" is incorrect. This will not reduce the latency of the API call as network latency is not the issue here, it is the latency of how long the API call takes to complete.

INCORRECT: "Increase the ALB idle timeout to allow the long-running requests to complete" is incorrect. The issue is not the connection being interrupted, it is that the API call takes a long time to complete.

INCORRECT: "Change the ALB to a Network Load Balancer (NLB) and use SSL/TLS termination" is incorrect. SSL/TLS termination is not of benefit here as the problem is not encryption or processing of encryption. The issue is API call latency.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 5

An application runs on EC2 instances in a private subnet behind an Application Load Balancer in a public subnet. The application is highly available and distributed across multiple AZs. The EC2 instances must make API calls to an internet-based service. How can the Solutions Architect enable highly available internet connectivity?

1. Create a NAT gateway and attach it to the VPC. Add a route to the gateway to each private subnet route table
2. Configure an internet gateway. Add a route to the gateway to each private subnet route table
3. Create a NAT instance in the private subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT instance
4. Create a NAT gateway in the public subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT gateway

Answer: 4

Explanation:

The only solution presented that actually works is to create a NAT gateway in the public subnet of each AZ. They must be created in the public subnet as they gain public IP addresses and use an internet gateway for internet access.

The route tables in the private subnets must then be configured with a route to the NAT gateway and then the EC2 instances will be able to access the internet (subject to security group configuration).

CORRECT: "Create a NAT gateway in the public subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT gateway" is the correct answer.

INCORRECT: "Create a NAT gateway and attach it to the VPC. Add a route to the gateway to each private subnet route table" is incorrect. You do not attach NAT gateways to VPCs, you add them to public subnets.

INCORRECT: "Configure an internet gateway. Add a route to the gateway to each private subnet route table" is incorrect. You cannot add a route to an internet gateway to a private subnet route table (private EC2 instances don't even have public IP addresses).

INCORRECT: "Create a NAT instance in the private subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT instance" is incorrect. You do not create NAT instances in private subnets, they must be created in public subnets.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 6

A legacy application is being migrated into AWS. The application has a large amount of data that is rarely accessed. When files are accessed they are retrieved sequentially. The application will be migrated onto an Amazon EC2 instance.

What is the LEAST expensive EBS volume type for this use case?

1. Cold HDD (sc1)
2. Provisioned IOPS SSD (io1)
3. General Purpose SSD (gp2)
4. Throughput Optimized HDD (st1)

Answer: 1

Explanation:

The cold HDD (sc1) EBS volume type is the lowest cost option that is suitable for this use case. The sc1 volume type is suitable for infrequently accessed data and use cases that are oriented towards throughput like sequential data access.

	Solid-state drives (SSD)		Hard disk drives (HDD)	
Volume type	General Purpose SSD (gp2)	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low-cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use cases	<ul style="list-style-type: none"> • Recommended for most workloads • System boot volumes • Virtual desktops 	<ul style="list-style-type: none"> • Critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MiB/s of throughput per volume • Large database workloads, 	<ul style="list-style-type: none"> • Streaming workloads requiring consistent, fast throughput at a low price • Big data 	<ul style="list-style-type: none"> • Throughput-oriented storage for large volumes of data that is infrequently accessed

CORRECT: "Cold HDD (sc1)" is the correct answer.

INCORRECT: "Provisioned IOPS SSD (io1)" is incorrect. This is the most expensive option and used for use cases that demand high IOPS.

INCORRECT: "General Purpose SSD (gp2)" is incorrect. This is a more expensive SSD volume type that is used for general use cases.

INCORRECT: "Throughput Optimized HDD (st1)" is incorrect. This is also used for throughput-oriented use cases however it is higher cost than sc1 and better for frequently accessed data.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 7

An application uses an Amazon RDS database and Amazon EC2 instances in a web tier. The web tier instances must not be directly accessible from the internet to improve security.

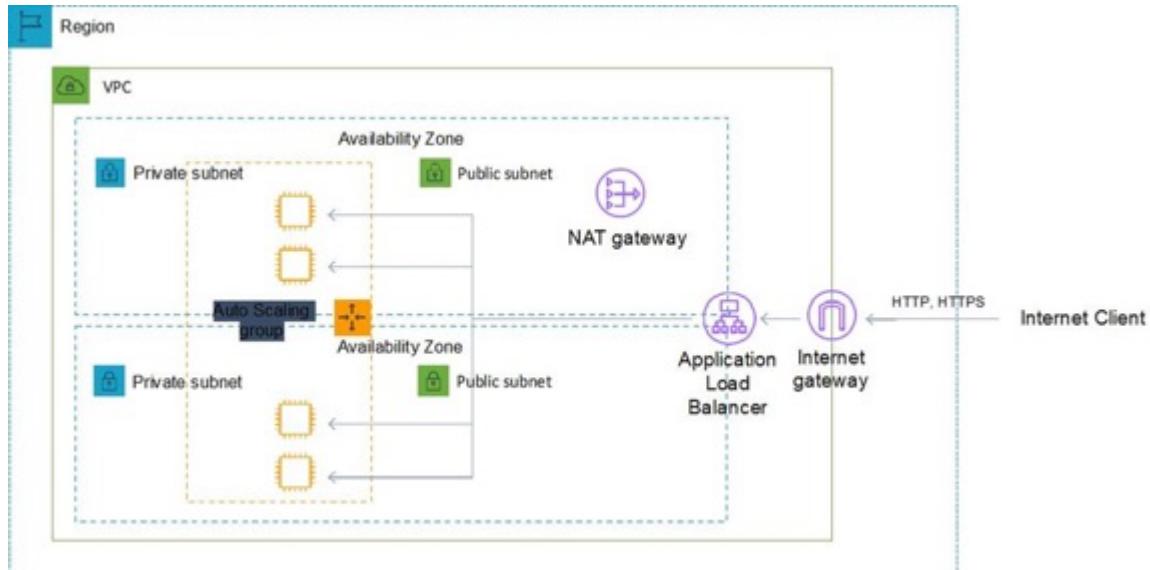
How can a Solutions Architect meet these requirements?

1. Launch the EC2 instances in a private subnet and create an Application Load Balancer in a public subnet
2. Launch the EC2 instances in a private subnet with a NAT gateway and update the route table
3. Launch the EC2 instances in a public subnet and use AWS WAF to protect the instances from internet-based attacks
4. Launch the EC2 instances in a public subnet and create an Application Load Balancer in a public subnet

Answer: 1

Explanation:

To prevent direct connectivity to the EC2 instances from the internet you can deploy your EC2 instances in a private subnet and have the ELB in a public subnet. To configure this you must enable a public subnet in the ELB that is in the same AZ as the private subnet.



CORRECT: "Launch the EC2 instances in a private subnet and create an Application Load Balancer in a public subnet" is the correct answer.

INCORRECT: "Launch the EC2 instances in a private subnet with a NAT gateway and update the route table" is incorrect. This configuration will not allow the application to be accessible from the internet, the aim is to only prevent direct access to the EC2 instances.

INCORRECT: "Launch the EC2 instances in a public subnet and use AWS WAF to protect the instances from internet-based attacks" is incorrect. With the EC2 instances in a public subnet, direct access from the internet is possible. It only takes a security group misconfiguration or software exploit and the instance becomes vulnerable to attack.

INCORRECT: "Launch the EC2 instances in a public subnet and create an Application Load Balancer in a public subnet" is incorrect. The EC2 instances should be launched in a private subnet.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 8

A company runs an application on premises that stores a large quantity of semi-structured data using key-value pairs. The application code will be migrated to AWS Lambda and a highly scalable solution is required for storing the data.

Which datastore will be the best fit for these requirements?

1. Amazon EFS
2. Amazon RDS MySQL
3. Amazon EBS
4. Amazon DynamoDB

Answer: 4

Explanation:

Amazon DynamoDB is a no-SQL database that stores data using key-value pairs. It is ideal for storing large amounts of semi-structured data and is also highly scalable. This is the best solution for storing this data based on the requirements in the scenario.

CORRECT: "Amazon DynamoDB" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect. The Amazon Elastic File System (EFS) is not suitable for storing key-value pairs.

INCORRECT: "Amazon RDS MySQL" is incorrect. Amazon Relational Database Service (RDS) is used for structured data as it is an SQL type of database.

INCORRECT: "Amazon EBS" is incorrect. Amazon Elastic Block Store (EBS) is a block-based storage system. You attach volumes to EC2 instances. It is not used for key-value pairs or to be used by Lambda functions.

References:

<https://aws.amazon.com/dynamodb/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

QUESTION 9

An application uses a MySQL database running on an Amazon EC2 instance. The application generates high I/O and constant writes to a single table on the database. Which Amazon EBS volume type will provide the MOST consistent performance and low latency?

1. General Purpose SSD (gp2)
2. Provisioned IOPS SSD (io1)
3. Throughput Optimized HDD (st1)
4. Cold HDD (sc1)

Answer: 2

Explanation:

The Provisioned IOPS SSD (io1) volume type will offer the most consistent performance and can be configured with the amount of IOPS required by the application. It will also provide the lowest latency of the options presented.

	Solid-state drives (SSD)		Hard disk drives (HDD)	
Volume type	General Purpose SSD (gp2)	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low-cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads

CORRECT: "Provisioned IOPS SSD (io1)" is the correct answer.

INCORRECT: "General Purpose SSD (gp2)" is incorrect. This is not the best solution for when you require high I/O, consistent performance and low latency.

INCORRECT: "Throughput Optimized HDD (st1)" is incorrect. This is a HDD type of disk and not suitable for low latency workloads that require consistent performance.

INCORRECT: "Cold HDD (sc1)" is incorrect. This is the lowest cost option and not suitable for frequently accessed workloads.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 10

A Solutions Architect needs to capture information about the traffic that reaches an Amazon Elastic Load Balancer. The information should include the source, destination, and protocol.

What is the most secure and reliable method for gathering this data?

1. Create a VPC flow log for each network interface associated with the ELB
2. Enable Amazon CloudTrail logging and configure packet capturing
3. Use Amazon CloudWatch Logs to review detailed logging information
4. Create a VPC flow log for the subnets in which the ELB is running

Answer: 1

Explanation:

You can use VPC Flow Logs to capture detailed information about the traffic going to and from your Elastic Load Balancer. Create a flow log for each network interface for your load balancer. There is one network interface per load balancer subnet.

CORRECT: "Create a VPC flow log for each network interface associated with the ELB" is the correct answer.

INCORRECT: "Enable Amazon CloudTrail logging and configure packet capturing" is incorrect. CloudTrail performs auditing of API actions, it does not do packet capturing.

INCORRECT: "Use Amazon CloudWatch Logs to review detailed logging information" is incorrect as this service does not record this information in CloudWatch logs.

INCORRECT: "Create a VPC flow log for the subnets in which the ELB is running" is incorrect as the more secure option is to use the ELB network interfaces.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>
<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-monitoring.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 11

The Solutions Architect in charge of a critical application must ensure the Amazon EC2 instances are able to be launched in another AWS Region in the event of a disaster.

What steps should the Solutions Architect take? (Select TWO.)

1. Launch instances in the second Region using the S3 API
2. Create AMIs of the instances and copy them to another Region
3. Enable cross-region snapshots for the Amazon EC2 instances
4. Launch instances in the second Region from the AMIs
5. Copy the snapshots using Amazon S3 cross-region replication

Answer: 2,4

Explanation:

You can create AMIs of the EC2 instances and then copy them across Regions. This provides a point-in-time copy of the state of the EC2 instance in the remote Region.

Once you've created AMIs of EC2 instances and copied them to the second Region, you can then launch the EC2 instances from the AMIs in that Region.

This is a good DR strategy as you have moved stateful EC2 instances to another Region.

CORRECT: "Create AMIs of the instances and copy them to another Region" is the correct answer.

CORRECT: "Launch instances in the second Region from the AMIs" is also a correct answer.

INCORRECT: "Launch instances in the second Region using the S3 API" is incorrect. Though snapshots (and EBS-backed AMIs) are stored on Amazon S3, you cannot actually access them using the S3 API. You must use the EC2 API.

INCORRECT: "Enable cross-region snapshots for the Amazon EC2 instances" is incorrect. You cannot enable "cross-region snapshots" as this is not a feature that currently exists.

INCORRECT: "Copy the snapshots using Amazon S3 cross-region replication" is incorrect. You cannot work with snapshots using Amazon S3 at all including leveraging the cross-region replication feature.

References:

<https://aws.amazon.com/blogs/aws/ebs-snapshot-copy/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 12

A company needs to ensure that they can failover between AWS Regions in the event of a disaster seamlessly with minimal downtime and data loss. The applications will run in an active-active configuration.

Which DR strategy should a Solutions Architect recommend?

1. Backup and restore
2. Pilot light
3. Warm standby
4. Multi-site

Answer: 4

Explanation:

A multi-site solution runs on AWS as well as on your existing on-site infrastructure in an active-active configuration. The data replication method that you employ will be determined by the recovery point that you choose. This is either Recovery Time Objective (the maximum allowable downtime before degraded operations are restored) or Recovery Point Objective (the maximum allowable time window whereby you will accept the loss of transactions during the DR process).

CORRECT: "Multi-site" is the correct answer.

INCORRECT: "Backup and restore" is incorrect. This is the lowest cost DR approach that simply entails creating online backups of all data and applications.

INCORRECT: "Pilot light" is incorrect. With a pilot light strategy a core minimum of services are running and the remainder are only brought online during a disaster recovery situation.

INCORRECT: "Warm standby" is incorrect. The term warm standby is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud.

References:

<https://aws.amazon.com/blogs/publicsector/rapidly-recover-mission-critical-systems-in-a-disaster/>

QUESTION 13

A company has launched a multi-tier application architecture. The web tier and database tier run on Amazon EC2 instances in private subnets within the same Availability Zone.

Which combination of steps should a Solutions Architect take to add high availability to this architecture? (Select TWO.)

1. Create new public subnets in the same AZ for high availability and move the web tier to the public subnets
2. Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs
3. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)
4. Create new private subnets in the same VPC but in a different AZ. Create a database using Amazon EC2 in one AZ
5. Create new private subnets in the same VPC but in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment

Answer: 2,5

Explanation:

The Solutions Architect can use Auto Scaling group across multiple AZs with an ALB in front to create an elastic and highly available architecture. Then, migrate the database to an Amazon RDS multi-AZ deployment to create HA for the database tier. This results in a fully redundant architecture that can withstand the failure of an availability zone.

CORRECT: "Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs" is a correct answer.

CORRECT: "Create new private subnets in the same VPC but in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment" is also a correct answer.

INCORRECT: "Create new public subnets in the same AZ for high availability and move the web tier to the public subnets" is

incorrect. If subnets share the same AZ they are not suitable for splitting your tier across them for HA as the failure of an AZ will take out both subnets.

INCORRECT: "Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)" is incorrect. The instances are in a single AZ so the Solutions Architect should create a new auto scaling group and launch instances across multiple AZs.

INCORRECT: "Create new private subnets in the same VPC but in a different AZ. Create a database using Amazon EC2 in one AZ" is incorrect. A database in a single AZ will not be highly available.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 14

An on-premises server runs a MySQL database and will be migrated to the AWS Cloud. The company require a managed solution that supports high availability and automatic failover in the event of the outage of an Availability Zone (AZ).

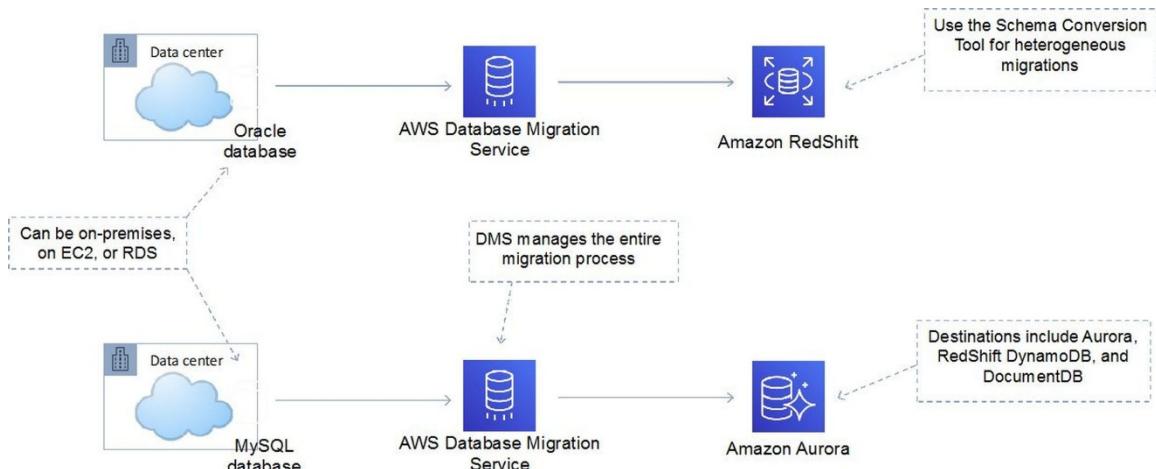
Which solution is the BEST fit for these requirements?

1. Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon RDS MySQL Multi-AZ deployment
2. Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon EC2 MySQL Multi-AZ deployment
3. Create a snapshot of the MySQL database server and use AWS DataSync to migrate the data Amazon S3. Launch a new Amazon RDS MySQL Multi-AZ deployment from the snapshot
4. Use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon RDS MySQL. Use the Schema Conversion Tool (SCT) to enable conversion from MySQL to Amazon RDS

Answer: 1

Explanation:

The AWS DMS service can be used to directly migrate the MySQL database to an Amazon RDS Multi-AZ deployment. The entire process can be online and is managed for you. There is no need to perform schema translation between MySQL and RDS (assuming you choose the MySQL RDS engine).



CORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon RDS MySQL Multi-AZ deployment" is the correct answer.

INCORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon EC2 MySQL Multi-AZ deployment" is incorrect as there is no such thing as "multi-AZ" on Amazon EC2 with MySQL, you must use RDS.

INCORRECT: "Create a snapshot of the MySQL database server and use AWS DataSync to migrate the data Amazon S3. Launch a new Amazon RDS MySQL Multi-AZ deployment from the snapshot" is incorrect. You cannot create a snapshot of a MySQL database server running on-premises.

INCORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon RDS MySQL. Use the Schema Conversion Tool (SCT) to enable conversion from MySQL to Amazon RDS" is incorrect. There is no need to convert the schema when migrating from MySQL to Amazon RDS (MySQL engine).

References:

<https://aws.amazon.com/rds/features/multi-az/>

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Introduction.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-database-migration-service/>

QUESTION 15

The database layer of an on-premises web application is being migrated to AWS. The database currently uses an in-memory cache. A Solutions Architect must deliver a solution that supports high availability and replication for the caching layer.

Which service should the Solutions Architect recommend?

1. Amazon ElastiCache Redis
2. Amazon RDS Multi-AZ
3. Amazon ElastiCache Memcached
4. Amazon DynamoDB

Answer: 1

Explanation:

Amazon ElastiCache Redis is an in-memory database cache and supports high availability through replicas and multi-AZ. The table below compares ElastiCache Redis with Memcached:

	Memcached	Redis (cluster mode disabled)	Redis (cluster mode enabled)
Data types	Simple	Complex	Complex
Data partitioning	Yes	No	Yes
Cluster is modifiable	Yes	Yes	No
Online re-sharding	No	No	3.2.10
Encryption	No	3.2.6	3.2.6
HIPAA Compliance	No	3.2.6	3.2.6
Multi-threaded	Yes	No	No
Node type upgrade	No	Yes	No
Engine upgrading	Yes	Yes	No
High availability (replication)	No	Yes	Yes
Automatic failover	No	Optional	Required

CORRECT: "Amazon ElastiCache Redis" is the correct answer.

INCORRECT: "Amazon ElasticCache Memcached" is incorrect as it does not support high availability or multi-AZ.

INCORRECT: "Amazon RDS Multi-AZ" is incorrect. This is not an in-memory database and it not suitable for use as a caching layer.

INCORRECT: "Amazon DynamoDB" is incorrect. DynamoDB is a non-relational database, you would not use it for a caching layer. Also, the in-memory, low-latency caching for DynamoDB is implemented using DynamoDB Accelerator (DAX).

References:

<https://aws.amazon.com/elasticache/redis-vs-memcached/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticsearch/>

QUESTION 16

A Solutions Architect has created an AWS Organization with several AWS accounts. Security policy requires that use of specific API actions are limited across all accounts. The Solutions Architect requires a method of centrally controlling these actions.

What is the SIMPLEST method of achieving the requirements?

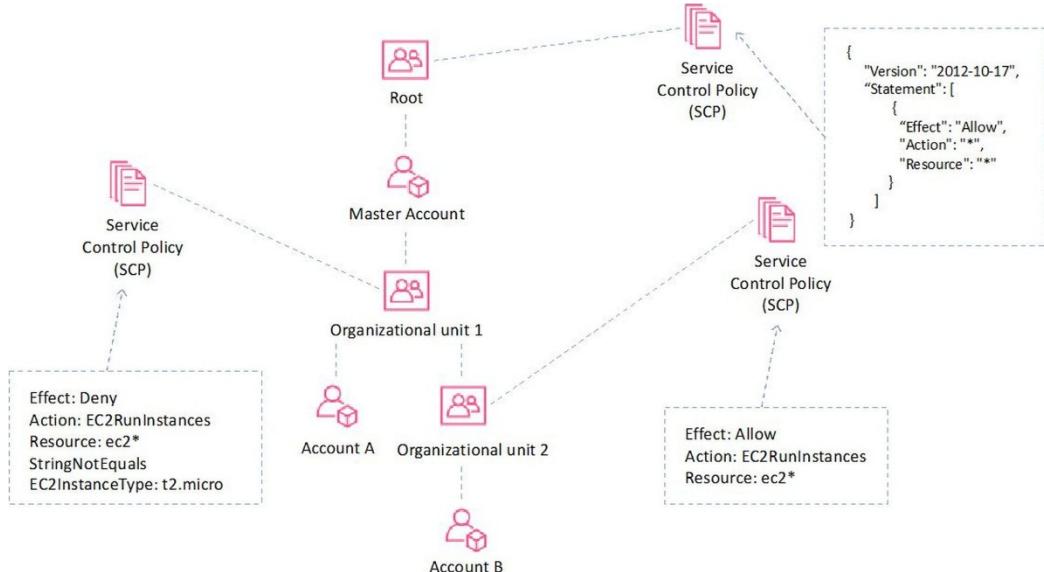
1. Create a Network ACL that limits access to the services or actions and attach it to all relevant subnets
2. Create an IAM policy in the root account and attach it to users and groups in each account
3. Create cross-account roles in each account to limit access to the services and actions that are allowed
4. Create a service control policy in the root organizational unit to deny access to the services or actions

Answer: 4

Explanation:

Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.

In the example below a policy in OU1 restricts all users from launching EC2 instance types other than a t2.micro:



CORRECT: "Create a service control policy in the root organizational unit to deny access to the services or actions" is the correct answer.

INCORRECT: "Create a Network ACL that limits access to the services or actions and attach it to all relevant subnets" is incorrect. Network ACLs control network traffic not API actions.

INCORRECT: "Create an IAM policy in the root account and attach it to users and groups in each account" is incorrect. This is not an efficient or centrally managed method of applying the security restrictions.

INCORRECT: "Create cross-account roles in each account to limit access to the services and actions that are allowed" is incorrect. This is another example of a complex and inefficient method of providing access across accounts and does not restrict API actions within the account.

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_about-scps.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-accounts/>

QUESTION 17

A company has a fleet of Amazon EC2 instances behind an Elastic Load Balancer (ELB) that are a mixture of c4.2xlarge instance types and c5.large instances. The load on the CPUs on the c5.large instances has been very high, often hitting 100% utilization, whereas the c4.2xlarge instances have been performing well.

What should a Solutions Architect recommend to resolve the performance issues?

1. Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances
2. Add all of the instances into a Placement Group
3. Change the configuration to use only c4.2xlarge instance types
4. Add more c5.large instances to spread the load more evenly

Answer: 3

Explanation:

The 2xlarge instance type provides more CPUs. The best answer is to use this instance type for all instances as the CPU utilization has been lower.

CORRECT: "Change the configuration to use only c4.2xlarge instance types" is the correct answer.

INCORRECT: "Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances" is incorrect. The weighted routing policy is a Route 53 feature that would not assist in this situation.

INCORRECT: "Add all of the instances into a Placement Group" is incorrect. A placement group helps provide low-latency connectivity between instances and would not help here.

INCORRECT: "Add more c5.large instances to spread the load more evenly" is incorrect. This would not help as this instance type is underperforming with high CPU utilization rates.

References:

<https://aws.amazon.com/ec2/instance-types/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 18

A Solutions Architect created a new IAM user account for a temporary employee who recently joined the company. The user does not have permissions to perform any actions, which statement is true about newly created users in IAM?

1. They are created with no permissions
2. They are created with limited permissions
3. They are created with full permissions
4. They are created with user privileges

Answer: 1

Explanation:

Every IAM user starts with no permissions.. In other words, by default, users can do nothing, not even view their own access keys. To give a user permission to do something, you can add the permission to the user (that is, attach a policy to the user). Or you can add the user to a group that has the intended permission.

CORRECT: "They are created with no permissions" is the correct answer.

INCORRECT: "They are created with limited permissions" is incorrect as they are created with no permissions.

INCORRECT: "They are created with full permissions" is incorrect as they are created with no permissions.

INCORRECT: "They are created with user privileges" is incorrect as they are created with no permissions.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_controlling.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

QUESTION 19

A government agency is using CloudFront for a web application that receives personally identifiable information (PII) from citizens. What feature of CloudFront applies an extra level of encryption at CloudFront edge locations to ensure the PII data is secured end-to-end?

1. Object invalidation
2. Field-level encryption
3. RTMP distribution
4. Origin access identity

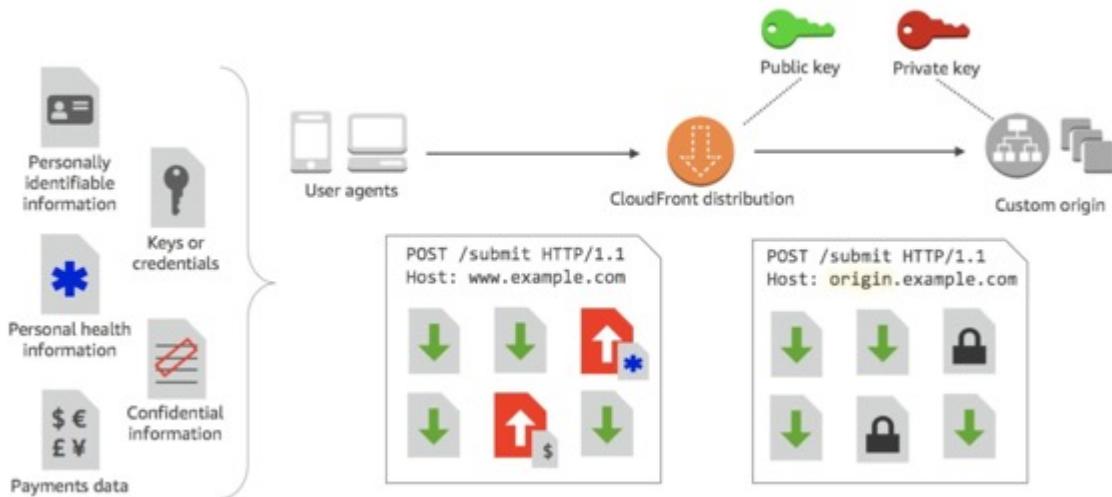
Answer: 2

Explanation:

With Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by using HTTPS. Field-level encryption adds an additional layer of security that lets you protect specific data throughout system processing so that only certain applications can see it.

Field-level encryption allows you to enable your users to securely upload sensitive information to your web servers. The sensitive information provided by your users is encrypted at the edge, close to the user, and remains encrypted throughout

your entire application stack. This encryption ensures that only applications that need the data—and have the credentials to decrypt it—are able to do so.



CORRECT: "Field-level encryption" is the correct answer.

INCORRECT: "Object invalidation" is incorrect. Object invalidation is a method to remove objects from the cache.

INCORRECT: "RTMP distribution" is incorrect. An RTMP distribution is a method of streaming media using Adobe Flash.

INCORRECT: "Origin access identity" is incorrect. Origin access identity applies to S3 bucket origins, not web servers.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/>

QUESTION 20

A company has multiple Amazon VPCs that are peered with each other. The company would like to use a single Elastic Load Balancer (ELB) to route traffic to multiple EC2 instances in peered VPCs within the same region. How can this be achieved?

1. This is not possible, the instances that an ELB routes traffic to must be in the same VPC
2. This is possible using the Classic Load Balancer (CLB) if using Instance IDs
3. This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets
4. This is not possible with ELB, you would need to use Route 53

Answer: 3

Explanation:

With ALB and NLB IP addresses can be used to register:

- Instances in a peered VPC.
- AWS resources that are addressable by IP address and port.
- On-premises resources linked to AWS through Direct Connect or a VPN connection.

CORRECT: "This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets" is the correct answer.

INCORRECT: "This is not possible, the instances that an ELB routes traffic to must be in the same VPC" is incorrect. Instances can be in peered VPCs.

INCORRECT: "This is possible using the Classic Load Balancer (CLB) if using Instance IDs" is incorrect. This is not possible with the CLB.

INCORRECT: "This is not possible with ELB, you would need to use Route 53" is incorrect. This is not true, as detailed above.

References:

<https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 21

Some data has become corrupted in an Amazon RDS database. A Solutions Architect plans to use point-in-time restore to recover the data to the last known good configuration. Which of the following statements is correct about restoring an RDS database to a specific point-in-time? (Select TWO.)

1. You can restore up to the last 5 minutes
2. Custom DB security groups are applied to the new DB instance
3. You can restore up to the last 1 minute
4. The default DB security group is applied to the new DB instance
5. The database restore overwrites the existing database

Answer: 1,4

Explanation:

You can restore a DB instance to a specific point in time, creating a new DB instance. When you restore a DB instance to a point in time, the default DB security group is applied to the new DB instance. If you need custom DB security groups applied to your DB instance, you must apply them explicitly using the AWS Management Console, the AWS CLI modify-db-instance command, or the Amazon RDS API ModifyDBInstance operation after the DB instance is available.

Restored DBs will always be a new RDS instance with a new DNS endpoint and you can restore up to the last 5 minutes.

CORRECT: "You can restore up to the last 5 minutes" is a correct answer.

CORRECT: "The default DB security group is applied to the new DB instance" is also a correct answer.

INCORRECT: "Custom DB security groups are applied to the new DB instance" is incorrect. Only default DB parameters and security groups are restored – you must manually associate all other DB parameters and SGs..

INCORRECT: "You can restore up to the last 1 minute" is incorrect. You can restore up to the last 5 minutes.

INCORRECT: "The database restore overwrites the existing database" is incorrect. You cannot restore from a DB snapshot to an existing DB – a new instance is created when you restore.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIT.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 22

An application is generating a large amount of clickstream events data that is being stored on S3. The business needs to understand customer behavior and want to run complex analytics queries against the data.

Which AWS service can be used for this requirement?

1. Amazon RedShift
2. Amazon Neptune
3. Amazon RDS
4. Amazon Kinesis Firehose

Answer: 1

Explanation:

Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools.

RedShift is used for running complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution.

With RedShift you can load data from Amazon S3 and perform analytics queries. RedShift Spectrum can analyze data directly in Amazon S3, but was not presented as an option.

CORRECT: "Amazon RedShift" is the correct answer.

INCORRECT: "Amazon Neptune" is incorrect. Amazon Neptune is a new product that offers a fully-managed Graph database.

INCORRECT: "Amazon RDS" is incorrect. RDS is a relational database that is used for transactional workloads not analytics workloads.

INCORRECT: "Amazon Kinesis Firehose" is incorrect. Amazon Kinesis Firehose processes streaming data, not data stored on S3.

References:

<https://aws.amazon.com/redshift/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>

QUESTION 23

A Solutions Architect is deploying a production application that will use several Amazon EC2 instances and run constantly on an ongoing basis. The application cannot be interrupted or restarted. Which EC2 pricing model would be best for this workload?

1. Reserved instances
2. On-demand instances
3. Spot instances
4. Flexible instances

Answer: 1

Explanation:

In this scenario for a stable process that will run constantly on an ongoing basis RIs will be the most affordable solution.

RIs provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. You have the flexibility to change families, OS types, and tenancies while benefitting from RI pricing when you use Convertible RIs.

CORRECT: "Reserved instances" is the correct answer.

INCORRECT: "On-demand instances" is incorrect. On-demand is useful for short term ad-hoc requirements for which the job cannot afford to be interrupted and are typically more expensive than Spot instances.

INCORRECT: "Spot instances" is incorrect. Spot is more suited to short term jobs that can afford to be interrupted and offer the lowest price of all options.

INCORRECT: "Flexible instances" is incorrect. There's no such thing as flexible instances.

References:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 24

A customer has requested some advice on how to implement security measures in their Amazon VPC. The client has recently been the victim of some hacking attempts. The client wants to implement measures to mitigate further threats. The client has explained that the attacks always come from the same small block of IP addresses.

What would be a quick and easy measure to help prevent further attacks?

1. Use a Security Group rule that denies connections from the block of IP addresses
2. Use CloudFront's DDoS prevention features

3. Create a Bastion Host restrict all connections to the Bastion Host only
4. Use a Network ACL rule that denies connections from the block of IP addresses

Answer: 4

Explanation:

With NACLs you can have permit and deny rules. Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic.

Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

CORRECT: "Use a Network ACL rule that denies connections from the block of IP addresses" is the correct answer.

INCORRECT: "Use a Security Group rule that denies connections from the block of IP addresses" is incorrect. With Security Groups you can only assign permit rules, you cannot assign deny rules.

INCORRECT: "Use CloudFront's DDoS prevention features" is incorrect. CloudFront does have DDoS prevention features but we don't know that this is a DDoS style of attack and CloudFront can only help where the traffic is using the CloudFront service to access cached content.

INCORRECT: "Create a Bastion Host restrict all connections to the Bastion Host only" is incorrect. A bastion host is typically used for admin purposes, allowing access to a single endpoint in the AWS cloud for administration using SSH/RDP. From the bastion instance you then connect to other EC2 instances in your subnets. This is not used as a method of adding security to production systems and cannot stop traffic from hitting application ports.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 25

An Amazon EC2 instance has been launched into an Amazon VPC. A Solutions Architect needs to ensure that instances have both a private and public DNS hostnames. Assuming settings were not changed during creation of the VPC, how will DNS hostnames be assigned by default? (Select TWO.)

1. In all VPCs instances no DNS hostnames will be assigned
2. In a non-default VPC instances will be assigned a public and private DNS hostname
3. In a default VPC instances will be assigned a public and private DNS hostname
4. In a non-default VPC instances will be assigned a private but not a public DNS hostname
5. In a default VPC instances will be assigned a private but not a public DNS hostname

Answer: 3,4

Explanation:

When you launch an instance into a default VPC, we provide the instance with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance.

When you launch an instance into a nondefault VPC, we provide the instance with a private DNS hostname and we might provide a public DNS hostname, depending on the DNS attributes you specify for the VPC and if your instance has a public IPv4 address.

All other statements are incorrect with default settings.

CORRECT: "In a default VPC instances will be assigned a public and private DNS hostname" is the correct answer.

CORRECT: "In a non-default VPC instances will be assigned a private but not a public DNS hostname" is the correct answer.

INCORRECT: "In all VPCs instances no DNS hostnames will be assigned" is incorrect as explained above.

INCORRECT: "In a non-default VPC instances will be assigned a public and private DNS hostname" is incorrect as explained above.

INCORRECT: "In a default VPC instances will be assigned a private but not a public DNS hostname" is incorrect as explained above.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 26

A fleet of Amazon EC2 instances running Linux will be launched in an Amazon VPC. An application development framework and some custom software must be installed on the instances. The installation will be initiated using some scripts. What feature enables a Solutions Architect to specify the scripts the software can be installed during the EC2 instance launch?

1. Metadata
2. Run Command
3. AWS Config
4. User Data

Answer: 4

Explanation:

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives

User data is data that is supplied by the user at instance launch in the form of a script and is limited to 16KB.

CORRECT: "User Data" is the correct answer.

INCORRECT: "Metadata" is incorrect. *Instance metadata* is data about your instance that you can use to configure or manage the running instance. Instance metadata is divided into categories, for example, host name, events, and security groups.

INCORRECT: "Run Command" is incorrect. The AWS Systems Manager run command is used to manage the configuration of existing instances by using remotely executed commands. User data is better for specifying scripts to run at startup.

INCORRECT: "AWS Config" is incorrect. This service is used to manage the configuration of AWS resources, it does not run scripts on instances.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 27

A company is investigating ways to analyze and process large amounts of data in the cloud faster, without needing to load or transform the data in a data warehouse. The data resides in Amazon S3.

Which AWS services would allow the company to query the data in place? (Select TWO.)

1. Amazon S3 Select
2. Amazon Kinesis Data Streams
3. Amazon Elasticsearch
4. Amazon RedShift Spectrum
5. Amazon SWF

Answer: 1,4

Explanation:

Amazon S3 Select is designed to help analyze and process data within an object in Amazon S3 buckets, faster and cheaper. It works by providing the ability to retrieve a subset of data from an object in Amazon S3 using simple SQL expressions

Amazon Redshift Spectrum allows you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required.

CORRECT: "Amazon S3 Select" is a correct answer.

CORRECT: "Amazon RedShift Spectrum" is also a correct answer.

INCORRECT: "Amazon Kinesis Data Streams" is incorrect. Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. It does not allow you to perform query-in-place operations on S3.

INCORRECT: "Amazon Elasticsearch" is incorrect. Amazon Elasticsearch Service, is a fully managed service that makes it easy for you to deploy, secure, operate, and scale Elasticsearch to search, analyze, and visualize data in real-time.

INCORRECT: "Amazon SWF" is incorrect. Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps.

References:

<https://aws.amazon.com/blogs/aws/s3-glacier-select/>

<https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-redshift-spectrum-is-now-available-in-four-additional-aws-regions-and-enhances-query-performance-in-all-available-aws-regions/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/>

QUESTION 28

A distribution method is required for some static files. The requests will mainly be GET requests and a high volume of GETs is expected, often exceeding 2000 per second. The files are currently stored in an S3 bucket. According to AWS best practices, how can performance be optimized?

1. Use cross-region replication to spread the load across regions
2. Use ElastiCache to cache the content
3. Integrate CloudFront with S3 to cache the content
4. Use S3 Transfer Acceleration

Answer: 3

Explanation:

Amazon S3 automatically scales to high request rates. For example, your application can achieve at least 3,500 PUT/POST/DELETE and 5,500 GET requests per second per prefix in a bucket. There are no limits to the number of prefixes in a bucket

If your workload is mainly sending GET requests, in addition to the preceding guidelines, you should consider using Amazon CloudFront for performance optimization. By integrating CloudFront with Amazon S3, you can distribute content to your users with low latency and a high data transfer rate.

CORRECT: "Integrate CloudFront with S3 to cache the content" is the correct answer.

INCORRECT: "Use cross-region replication to spread the load across regions" is incorrect. Cross-region replication creates a replica copy in another region but should not be used for spreading read requests across regions. There will be 2 S3 endpoints and CRR is not designed for 2 way sync so this would not work well.

INCORRECT: "Use ElastiCache to cache the content" is incorrect. ElastiCache is used for caching database content not S3 content.

INCORRECT: "Use S3 Transfer Acceleration" is incorrect. Transfer Acceleration is used to accelerate object **uploads** to S3 over long distances (latency).

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 29

An Auto Scaling group of Amazon EC2 instances behind an Elastic Load Balancer (ELB) is running in an Amazon VPC. Health checks are configured on the ASG to use EC2 status checks. The ELB has determined that an EC2 instance is unhealthy and has removed it from service. A Solutions Architect noticed that the instance is still running and has not been terminated by EC2 Auto Scaling.

What would be an explanation for this behavior?

1. The ASG is waiting for the cooldown timer to expire before terminating the instance
2. Connection draining is enabled and the ASG is waiting for in-flight requests to complete
3. The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service
4. The health check grace period has not yet expired

Answer: 3

Explanation:

If using an ELB it is best to enable ELB health checks as otherwise EC2 status checks may show an instance as being healthy that the ELB has determined is unhealthy. In this case the instance will be removed from service by the ELB but will not be terminated by Auto Scaling

More information on ASG health checks:

- By default uses EC2 status checks.
- Can also use ELB health checks and custom health checks.
- ELB health checks are in addition to the EC2 status checks.
- If any health check returns an unhealthy status the instance will be terminated.
- With ELB an instance is marked as unhealthy if ELB reports it as OutOfService
- A healthy instance enters the InService state.
- If an instance is marked as unhealthy it will be scheduled for replacement.
- If connection draining is enabled, Auto Scaling waits for in-flight requests to complete or timeout before terminating instances.
- The health check grace period allows a period of time for a new instance to warm up before performing a health check (300 seconds by default).

CORRECT: "The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service" is the correct answer.

INCORRECT: "The ASG is waiting for the cooldown timer to expire before terminating the instance" is incorrect as the ASG does not wait for the cooldown time to expire.

INCORRECT: "Connection draining is enabled and the ASG is waiting for in-flight requests to complete" is incorrect. Connection draining is not the correct answer as the ELB has taken the instance out of service so there are no active connections.

INCORRECT: "The health check grace period has not yet expired" is incorrect. The health check grace period allows a period of time for a new instance to warm up before performing a health check.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroupLifecycle.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 30

A financial services company regularly runs an analysis of the day's transaction costs, execution reporting, and market performance. The company currently uses third-party commercial software for provisioning, managing, monitoring, and scaling the computing jobs which utilize a large fleet of EC2 instances.

The company is seeking to reduce costs and utilize AWS services. Which AWS service could be used in place of the third-party software?

1. Amazon Athena
2. AWS Systems Manager
3. Amazon Lex
4. AWS Batch

Answer: 4

Explanation:

AWS Batch eliminates the need to operate third-party commercial or open source batch processing solutions. There is no batch software or servers to install or manage. AWS Batch manages all the infrastructure for you, avoiding the complexities of provisioning, managing, monitoring, and scaling your batch computing jobs.

CORRECT: "AWS Batch" is the correct answer.

INCORRECT: "Amazon Athena" is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.

INCORRECT: "AWS Systems Manager" is incorrect. AWS Systems Manager gives you visibility and control of your infrastructure on AWS.

INCORRECT: "Amazon Lex" is incorrect. Amazon Lex is a service for building conversational interfaces into any application using voice and text.

References:

<https://aws.amazon.com/batch/>

QUESTION 31

A customer is deploying services in a hybrid cloud model. The customer has mandated that data is transferred directly between cloud data centers, bypassing ISPs.

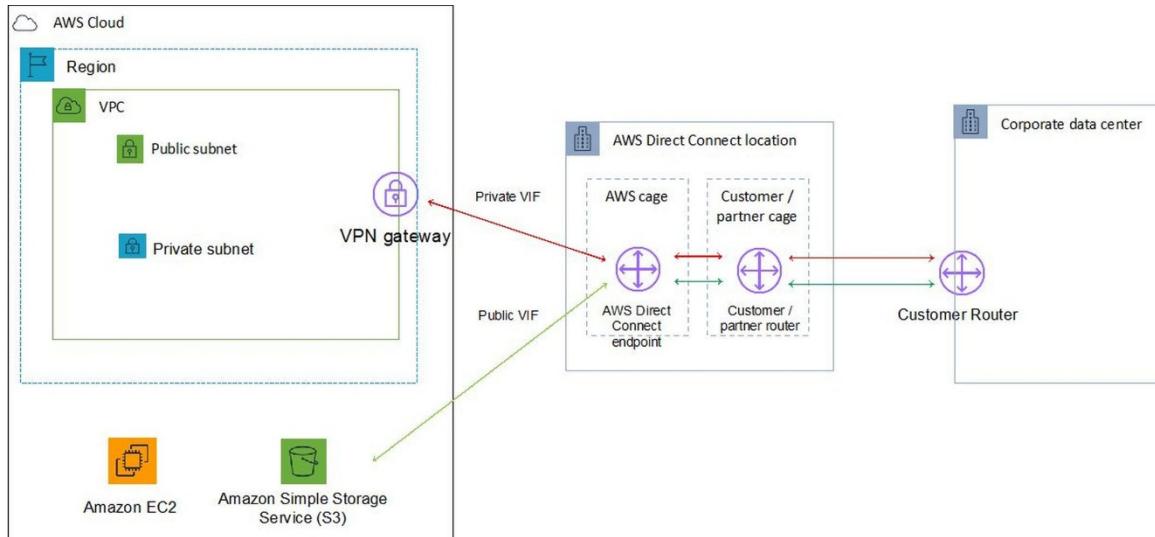
Which AWS service can be used to enable hybrid cloud connectivity?

1. AWS Direct Connect
2. Amazon VPC
3. IPSec VPN
4. Amazon Route 53

Answer: 1

Explanation:

With AWS Direct Connect, you can connect to all your AWS resources in an AWS Region, transfer your business-critical data directly from your datacenter, office, or colocation environment into and from AWS, bypassing your Internet service provider and removing network congestion.



CORRECT: "AWS Direct Connect" is the correct answer.

INCORRECT: "Amazon VPC" is incorrect. Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

INCORRECT: "IPSec VPN" is incorrect. An IPSec VPN can be used to connect to AWS however it does not bypass the ISPs or Internet.

INCORRECT: "Amazon Route 53" is incorrect. Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service.

References:

<https://aws.amazon.com/directconnect/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/>

QUESTION 32

An Amazon Elastic File System (EFS) has been created to store data that will be accessed by a large number of Amazon EC2 instances. The data is sensitive and a Solutions Architect is creating a design for security measures to protect the data. It is required that network traffic is restricted correctly based on firewall rules and access from hosts is restricted by user or group.

How can this be achieved with Amazon EFS? (Select TWO.)

1. Use POSIX permissions to control access from hosts by user or group
2. Use AWS Web Application Firewall (WAF) to protect EFS
3. Use EFS Security Groups to control network traffic
4. Use Network ACLs to control the traffic
5. Use IAM groups to control access by user or group

Answer: 1,3

Explanation:

You can control who can administer your file system using IAM. You can control access to files and directories with POSIX-compliant user and group-level permissions. POSIX permissions allows you to restrict access from hosts by user and group. EFS Security Groups act as a firewall, and the rules you add define the traffic flow.

CORRECT: "Use POSIX permissions to control access from hosts by user or group" is the correct answer.

CORRECT: "Use EFS Security Groups to control network traffic" is the correct answer.

INCORRECT: "Use AWS Web Application Firewall (WAF) to protect EFS" is incorrect. You cannot use AWS WAF to protect EFS

data using users and groups.

INCORRECT: "Use Network ACLs to control the traffic" is incorrect. You use EFS Security Groups to control network traffic to EFS, not Network ACLs.

INCORRECT: "Use IAM groups to control access by user or group" is incorrect. You do not use IAM to control access to files and directories by user and group, but you can use IAM to control who can administer the file system configuration.

References:

<https://aws.amazon.com/efs/features/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/>

QUESTION 33

A large multi-national client has requested a design for a multi-region database. The master database will be in the EU (Frankfurt) region and databases will be located in 4 other regions to service local read traffic. The database should be a managed service including the replication.

The solution should be cost-effective and secure. Which AWS service can deliver these requirements?

1. RDS with Multi-AZ
2. EC2 instances with EBS replication
3. RDS with cross-region Read Replicas
4. ElastiCache with Redis and clustering mode enabled

Answer: 3

Explanation:

Amazon RDS Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas are for workload sharing and offloading. Read replicas can be in another region (uses asynchronous replication). This solution will enable better performance for users in the other AWS regions for database queries and is a managed service.

CORRECT: "RDS with cross-region Read Replicas" is the correct answer.

INCORRECT: "RDS with Multi-AZ" is incorrect. RDS with Multi-AZ is within a region only

INCORRECT: "EC2 instances with EBS replication" is incorrect. EC2 instances with EBS replication is not a suitable solution.

INCORRECT: "ElastiCache with Redis and clustering mode enabled" is incorrect. ElastiCache is an in-memory key/value store database (more OLAP than OLTP) and is not suitable for this scenario. Clustering mod is only available within the same region.

References:

<https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/>

QUESTION 34

A Solutions Architect is designing the system monitoring and deployment layers of a serverless application. The system monitoring layer will manage system visibility through recording logs and metrics and the deployment layer will deploy the application stack and manage workload changes through a release management process.

The Architect needs to select the most appropriate AWS services for these functions. Which services and frameworks should be used for the system monitoring and deployment layers? (Select TWO.)

1. Use AWS CloudTrail for consolidating system and application logs and monitoring custom metrics
2. Use AWS X-Ray to package, test, and deploy the serverless application stack
3. Use AWS SAM to package, test, and deploy the serverless application stack
4. Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics
5. Use AWS Lambda to package, test, and deploy the serverless application stack

Answer: 3,4

Explanation:

AWS Serverless Application Model (AWS SAM) is an extension of AWS CloudFormation that is used to package, test, and deploy serverless applications.

With Amazon CloudWatch, you can access system metrics on all the AWS services you use, consolidate system and application level logs, and create business key performance indicators (KPIs) as custom metrics for your specific needs.

CORRECT: "Use AWS SAM to package, test, and deploy the serverless application stack" is a correct answer.

CORRECT: "Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics" is also a correct answer.

INCORRECT: "Use AWS CloudTrail for consolidating system and application logs and monitoring custom metrics" is incorrect as CloudTrail is used for auditing not performance monitoring.

INCORRECT: "Use AWS X-Ray to package, test, and deploy the serverless application stack" is incorrect. AWS X-Ray lets you analyze and debug serverless applications by providing distributed tracing and service maps to easily identify performance bottlenecks by visualizing a request end-to-end.

INCORRECT: "Use AWS Lambda to package, test, and deploy the serverless application stack" is incorrect. AWS Lambda is used for executing your code as functions, it is not used for packaging, testing and deployment. AWS Lambda is used with AWS SAM.

References:

https://docs.aws.amazon.com/lambda/latest/dg/serverless_app.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/>

QUESTION 35

One of the departments in a company has been generating a large amount of data on Amazon S3 and costs are increasing. Data older than 90 days is rarely accessed but must be retained for several years. If this data does need to be accessed at least 24 hours notice is provided.

How can a Solutions Architect optimize the costs associated with storage of this data whilst ensuring it is accessible if required?

1. Implement archival software that automatically moves the data to tape
2. Use S3 lifecycle policies to move data to the STANDARD_IA storage class
3. Use S3 lifecycle policies to move data to GLACIER after 90 days
4. Select the older data and manually migrate it to GLACIER

Answer: 3

Explanation:

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Transition actions define when objects transition to another storage class.

For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.

GLACIER retrieval times:

- Standard retrieval is 3-5 hours which is well within the requirements here.
- You can use Expedited retrievals to access data in 1 – 5 minutes.
- You can use Bulk retrievals to access up to petabytes of data in approximately 5 – 12 hours.

CORRECT: "Use S3 lifecycle policies to move data to GLACIER after 90 days" is the correct answer.

INCORRECT: "Implement archival software that automatically moves the data to tape" is incorrect as this solution can be fully automated using lifecycle policies.

INCORRECT: "Use S3 lifecycle policies to move data to the STANDARD_IA storage class" is incorrect. STANDARD_IA is good for infrequently accessed data and provides faster access times than GLACIER but is more expensive so not the best option here.

INCORRECT: "Select the older data and manually migrate it to GLACIER" is incorrect as a lifecycle policy can automate the process.

References:

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

<https://aws.amazon.com/about-aws/whats-new/2016/11/access-your-amazon-glacier-data-in-minutes-with-new-retrieval-options/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 36

A Solutions Architect enabled Access Logs on an Application Load Balancer (ALB) and needs to process the log files using a hosted Hadoop service. What configuration changes and services can be leveraged to deliver this requirement?

1. Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files
2. Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files
3. Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files
4. Configure Access Logs to be delivered to S3 and use EMR for processing the log files

Answer: 4

Explanation:

Access Logs can be enabled on ALB and configured to store data in an S3 bucket. Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3.

CORRECT: "Configure Access Logs to be delivered to S3 and use EMR for processing the log files" is the correct answer.

INCORRECT: "Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files" is incorrect. EC2 does not provide a hosted Hadoop service.

INCORRECT: "Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files" is incorrect. You cannot configure access logs to be delivered to DynamoDB.

INCORRECT: "Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files" is incorrect. Kinesis does not provide a hosted Hadoop service.

References:

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 37

A web application receives order processing information from customers and places the messages on an Amazon SQS queue. A fleet of Amazon EC2 instances are configured to pick up the messages, process them, and store the results in a DynamoDB table. The current configuration has been resulting in a large number of empty responses to **ReceiveMessage** API requests.

A Solutions Architect needs to eliminate empty responses to reduce operational overhead. How can this be done?

1. Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once
2. Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received
3. Configure Long Polling to eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response
4. Configure Short Polling to eliminate empty responses by reducing the length of time a connection request remains open

Answer: 3

Explanation:

The correct answer is to use Long Polling which will eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response.

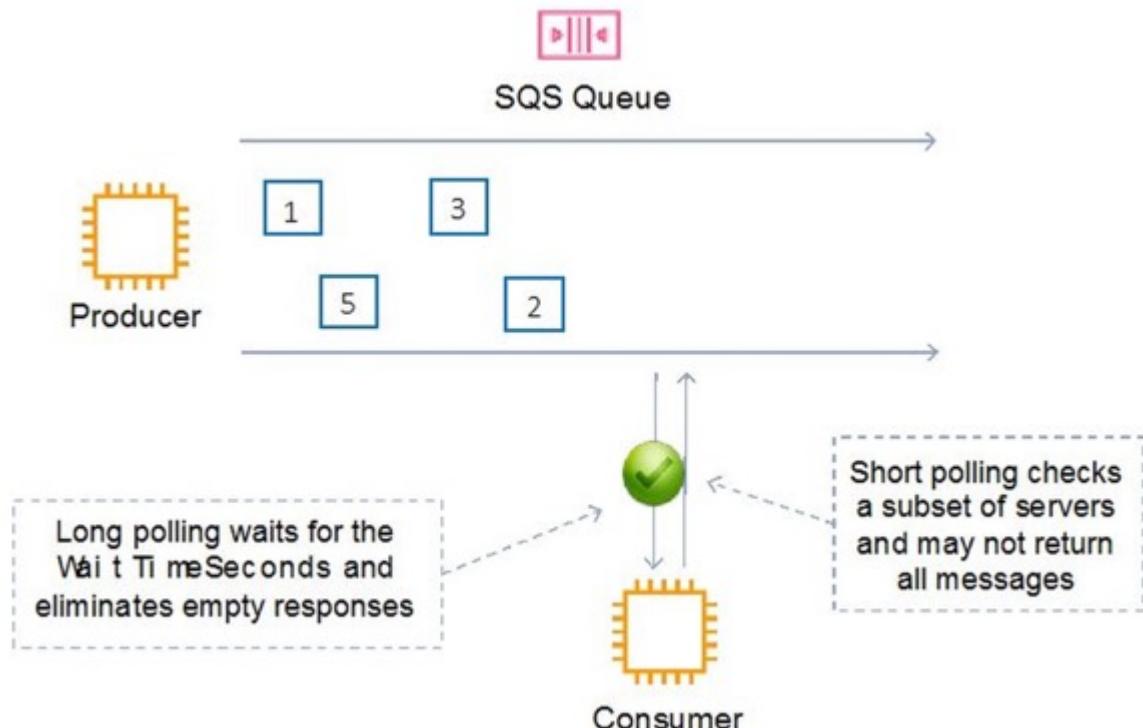
The problem does not relate to the order in which the messages are processed in and there are no concerns over messages being delivered more than once so it doesn't matter whether you use a FIFO or standard queue.

Long Polling:

- Uses fewer requests and reduces cost.
- Eliminates false empty responses by querying all servers.
- SQS waits until a message is available in the queue before sending a response.

Short Polling:

- Does not wait for messages to appear in the queue.
- It queries only a subset of the available servers for messages (based on weighted random execution).
- Short polling is the default.
- `ReceiveMessageWaitTime` is set to 0.



CORRECT: "Configure Long Polling to eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response" is the correct answer.

INCORRECT: "Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once" is incorrect as explained above.

INCORRECT: "Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received" is incorrect as explained above.

INCORRECT: "Configure Short Polling to eliminate empty responses by reducing the length of time a connection request remains open" is incorrect as explained above.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-short-and-long-polling.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 38

A Solutions Architect has created an AWS account and selected the Asia Pacific (Sydney) region. Within the default VPC there is a default security group. What settings are configured within this security group by default? (Select TWO.)

1. There is an inbound rule that allows all traffic from the security group itself
2. There is an inbound rule that allows all traffic from any address
3. There is an outbound rule that allows all traffic to the security group itself
4. There is an outbound rule that allows all traffic to all addresses
5. There is an outbound rule that allows traffic to the VPC router

Answer: 1,4

Explanation:

Default security groups have inbound allow rules (allowing traffic from within the group) whereas custom security groups do not have inbound allow rules (all inbound traffic is denied by default). All outbound traffic is allowed by default in custom and default security groups.

CORRECT: "There is an inbound rule that allows all traffic from the security group itself" is a correct answer.

CORRECT: "There is an outbound rule that allows all traffic to all addresses" is also a correct answer.

INCORRECT: "There is an inbound rule that allows all traffic from any address" is incorrect as explained above.

INCORRECT: "There is an outbound rule that allows all traffic to the security group itself" is incorrect as explained above.

INCORRECT: "There is an outbound rule that allows traffic to the VPC router" is incorrect as explained above.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 39

A company is deploying a new two-tier web application that uses EC2 web servers and a DynamoDB database backend. An Internet facing ELB distributes connections between the web servers.

The Solutions Architect has created a security group for the web servers and needs to create a security group for the ELB. What rules should be added? (Select TWO.)

1. Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group
2. Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway
3. Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR
4. Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0
5. Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32

Answer: 1,4

Explanation:

An inbound rule should be created for the relevant protocols (HTTP/HTTPS) and the source should be set to any address (0.0.0.0/0).

The outbound rule should forward the relevant protocols (HTTP/HTTPS) and the destination should be set to the web server security group.

Note that on the web server security group you'd want to add an Inbound rule allowing HTTP/HTTPS from the ELB security group.

CORRECT: "Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group" is a correct answer.

CORRECT: "Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0" is also a correct answer.

INCORRECT: "Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway" is incorrect as the relevant protocol should be specified and the destination should be the web server security group.

INCORRECT: "Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR" is incorrect. Using the VPC CIDR would not be secure and you cannot specify an Internet Gateway in a security group (not that you'd want to anyway).

INCORRECT: "Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32" is incorrect. The address 0.0.0.0/32 is incorrect as the 32 mask means an exact match is required (0.0.0.0).

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 40

A development team needs to run up a few lab servers on a weekend for a new project. The servers will need to run uninterrupted for a few hours. Which EC2 pricing option would be most suitable?

1. Spot
2. Reserved
3. On-Demand
4. Dedicated Instances

Answer: 3

Explanation:

On-Demand pricing ensures that instances will not be terminated and is the most economical option. Use on-demand for ad-hoc requirements where you cannot tolerate interruption.

CORRECT: "On-Demand" is the correct answer.

INCORRECT: "Spot" is incorrect. Spot pricing may be the most economical option for a short duration over a weekend but you may have the instances terminated by AWS and there is a requirement that the servers run uninterrupted.

INCORRECT: "Reserved" is incorrect. Reserved pricing provides a reduced cost for a contracted period (1 or 3 years), and is not suitable for ad hoc requirements.

INCORRECT: "Dedicated instances" is incorrect. Dedicated instances run on hardware that's dedicated to a single customer and are more expensive than regular On-Demand instances.

References:

<https://aws.amazon.com/ec2/pricing/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 41

A Solutions Architect has logged into an Amazon EC2 Linux instance using SSH and needs to determine a few pieces of information including what IAM role is assigned, the instance ID and the names of the security groups that are assigned to the instance.

From the options below, what would be the best source of this information?

1. Metadata
2. Tags
3. User data
4. Parameters

Answer: 1

Explanation:

Instance metadata is data about your instance that you can use to configure or manage the running instance. Instance metadata is divided into categories, for example, host name, events, and security groups.

Instance metadata is available at <http://169.254.169.254/latest/meta-data>.

CORRECT: "Metadata" is the correct answer.

INCORRECT: "Tags" is incorrect. Tags are used to categorize and label resources.

INCORRECT: "User data" is incorrect. User data is used to configure the system at launch time and specify scripts.

INCORRECT: "Parameters" is incorrect. Parameters are used in databases.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 42

An Amazon EC2 instance is generating very high packets-per-second and performance of the application stack is being impacted. A Solutions Architect needs to determine a resolution to the issue that results in improved performance.

Which action should the Architect take?

1. Configure a RAID 1 array from multiple EBS volumes
2. Create a placement group and put the EC2 instance in it
3. Use enhanced networking
4. Add multiple Elastic IP addresses to the instance

Answer: 3

Explanation:

Enhanced networking provides higher bandwidth, higher packet-per-second (PPS) performance, and consistently lower inter-instance latencies. If your packets-per-second rate appears to have reached its ceiling, you should consider moving to enhanced networking because you have likely reached the upper thresholds of the VIF driver. It is only available for certain instance types and only supported in VPC. You must also launch an HVM AMI with the appropriate drivers

AWS currently supports enhanced networking capabilities using SR-IOV. SR-IOV provides direct access to network adapters, provides higher performance (packets-per-second) and lower latency.

CORRECT: "Use enhanced networking" is the correct answer.

INCORRECT: "Configure a RAID 1 array from multiple EBS volumes" is incorrect. You do not need to create a RAID 1 array (which is more for redundancy than performance anyway).

INCORRECT: "Create a placement group and put the EC2 instance in it" is incorrect. A placement group is used to increase network performance between instances. In this case there is only a single instance so it won't help.

INCORRECT: "Add multiple Elastic IP addresses to the instance" is incorrect. Adding multiple IP addresses is not a way to increase performance of the instance as the same amount of bandwidth is available to the Elastic Network Interface (ENI).

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/>

QUESTION 43

A company runs a web-based application that uses Amazon EC2 instances for the web front-end and Amazon RDS for the database back-end. The web application writes transaction log files to an Amazon S3 bucket and the quantity of files is becoming quite large. It is acceptable to retain the most recent 60 days of log files and permanently delete the rest.

Which action can a Solutions Architect take to enable this to happen automatically?

1. Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old
2. Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old
3. Use an S3 bucket policy that deletes objects that are more than 60 days old
4. Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class

Answer: 1

Explanation:

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

- Transition actions—Define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.
- Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf.

CORRECT: "Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old" is the correct answer.

INCORRECT: "Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old" is incorrect as the automated method is to use object expiration.

INCORRECT: "Use an S3 bucket policy that deletes objects that are more than 60 days old" is incorrect as you cannot do this with bucket policies.

INCORRECT: "Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class" is incorrect. Moving logs to Glacier may save cost but the question requests that the files are permanently deleted.

References:

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

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 44

A Solutions Architect needs to upload a large (2GB) file to an S3 bucket. What is the recommended way to upload a single large file to an S3 bucket?

1. Use AWS Import/Export
2. Use Multipart Upload
3. Use a single PUT request to upload the large file
4. Use Amazon Snowball

Answer: 2

Explanation:

In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.

CORRECT: "Use Multipart Upload" is the correct answer.

INCORRECT: "Use AWS Import/Export" is incorrect. AWS Import/Export is a service in which you send in HDDs with data on to AWS and they import your data into S3. It is not used for single files.

INCORRECT: "Use a single PUT request to upload the large file" is incorrect. The largest object that can be uploaded in a single PUT is 5 gigabytes.

INCORRECT: "Use Amazon Snowball" is incorrect. Snowball is used for migrating large quantities (TB/PB) of data into AWS, it is overkill for this requirement.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 45

Several Amazon EC2 Spot instances are being used to process messages from an Amazon SQS queue and store results in an Amazon DynamoDB table. Shortly after picking up a message from the queue AWS terminated the Spot instance. The Spot

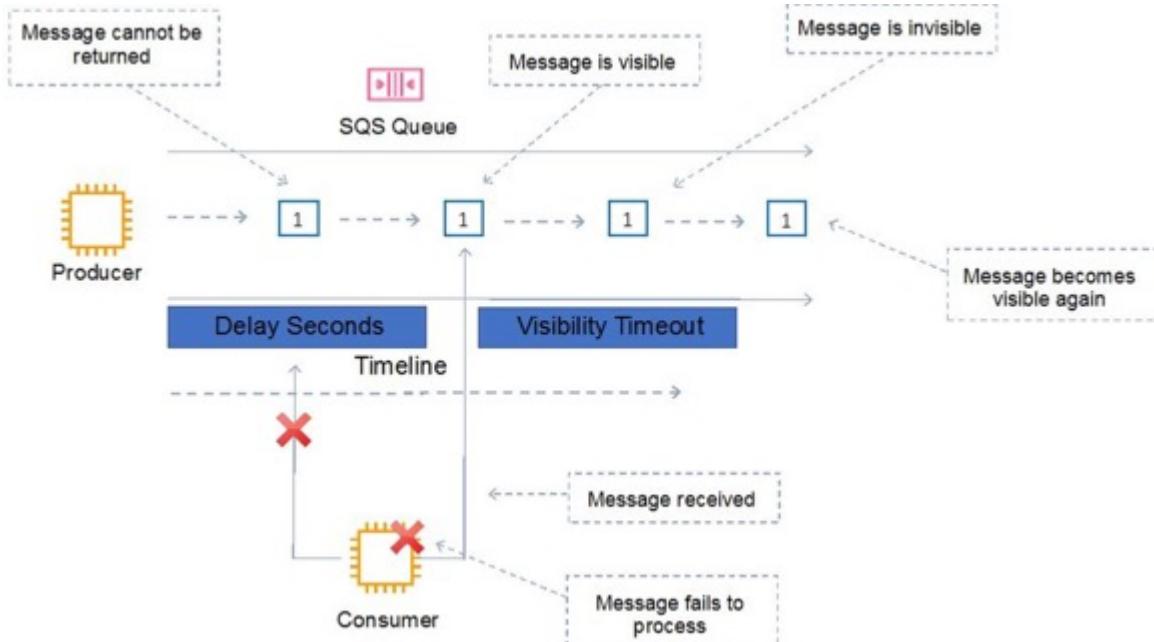
instance had not finished processing the message. What will happen to the message?

1. The message will become available for processing again after the visibility timeout expires
2. The message will be lost as it would have been deleted from the queue when processed
3. The message will remain in the queue and be immediately picked up by another instance
4. The results may be duplicated in DynamoDB as the message will likely be processed multiple times

Answer: 1

Explanation:

The visibility timeout is the amount of time a message is invisible in the queue after a reader picks up the message. If a job is processed within the visibility timeout the message will be deleted. If a job is not processed within the visibility timeout the message will become visible again (could be delivered twice). The maximum visibility timeout for an Amazon SQS message is 12 hours.



CORRECT: "The message will become available for processing again after the visibility timeout expires" is the correct answer.

INCORRECT: "The message will be lost as it would have been deleted from the queue when processed" is incorrect. The message will not be lost and will not be immediately picked up by another instance.

INCORRECT: "The message will remain in the queue and be immediately picked up by another instance" is incorrect. As mentioned above it will be available for processing in the queue again after the timeout expires.

INCORRECT: "The results may be duplicated in DynamoDB as the message will likely be processed multiple times" is incorrect. As the instance had not finished processing the message it should only be fully processed once. Depending on your application process however it is possible some data was written to DynamoDB.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/>

QUESTION 46

A company is transitioning their web presence into the AWS cloud. As part of the migration the company will be running a web application both on-premises and in AWS for a period of time. During the period of co-existence the client would like 80% of the traffic to hit the AWS-based web servers and 20% to be directed to the on-premises web servers.

What method can a Solutions Architect use to distribute traffic as requested?

1. Use Route 53 with a weighted routing policy and configure the respective weights
2. Use Route 53 with a simple routing policy
3. Use an Application Load Balancer to distribute traffic based on IP address
4. Use a Network Load Balancer to distribute traffic based on Instance ID

Answer: 1

Explanation:

Route 53 weighted routing policy is similar to simple but you can specify a weight per IP address. You create records that have the same name and type and assign each record a relative weight which is a numerical value that favours one IP over another (values must total 100). To stop sending traffic to a resource you can change the weight of the record to 0.

CORRECT: "Use Route 53 with a weighted routing policy and configure the respective weights" is the correct answer.

INCORRECT: "Use Route 53 with a simple routing policy" is incorrect as this will not split traffic based on weights as required.

INCORRECT: "Use an Application Load Balancer to distribute traffic based on IP address" is incorrect. Application Load Balancer can distribute traffic to AWS and on-premise resources using IP addresses but cannot be used to distribute traffic in a weighted manner.

INCORRECT: "Use a Network Load Balancer to distribute traffic based on Instance ID" is incorrect. Network Load Balancer can distribute traffic to AWS and on-premise resources using IP addresses (not Instance IDs).

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/>

QUESTION 47

A Solutions Architect has created a new Network ACL in an Amazon VPC. No rules have been created. Which of the statements below are correct regarding the default state of the Network ACL? (Select TWO.)

1. There is a default inbound rule allowing traffic from the VPC CIDR block
2. There is a default outbound rule allowing traffic to the Internet Gateway
3. There is a default outbound rule allowing all traffic
4. There is a default inbound rule denying all traffic
5. There is a default outbound rule denying all traffic

Answer: 4,5

Explanation:

A VPC automatically comes with a default network ACL which allows all inbound/outbound traffic. A custom NACL denies all traffic both inbound and outbound by default.

Network ACL's function at the subnet level and you can have permit and deny rules. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic.

Network ACLs are stateless so responses are subject to the rules for the direction of traffic. NACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet.

CORRECT: "There is a default inbound rule denying all traffic" is a correct answer.

CORRECT: "There is a default outbound rule denying all traffic" is also a correct answer.

INCORRECT: "There is a default inbound rule allowing traffic from the VPC CIDR block" is incorrect as inbound traffic is not allowed from anywhere by default.

INCORRECT: "There is a default outbound rule allowing traffic to the Internet Gateway" is incorrect as outbound traffic is not allowed to anywhere by default.

INCORRECT: "There is a default outbound rule allowing all traffic" is incorrect as all traffic is denied.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 48

A company needs to capture detailed information about all HTTP requests that are processed by their Internet facing Application Load Balancer (ALB). The company requires information on the requester, IP address, and request type for analyzing traffic patterns to better understand their customer base.

Which actions should a Solutions Architect recommend?

1. Configure metrics in CloudWatch for the ALB
2. Enable EC2 detailed monitoring
3. Enable Access Logs and store the data on S3
4. Use CloudTrail to capture all API calls made to the ALB

Answer: 3

Explanation:

You can enable access logs on the ALB and this will provide the information required including requester, IP, and request type. Access logs are not enabled by default. You can optionally store and retain the log files on S3.

CORRECT: "Enable Access Logs and store the data on S3" is the correct answer.

INCORRECT: "Configure metrics in CloudWatch for the ALB" is incorrect. CloudWatch is used for performance monitoring and CloudTrail is used for auditing API access..

INCORRECT: "Enable EC2 detailed monitoring" is incorrect. Enabling EC2 detailed monitoring will not capture the information requested.

INCORRECT: Use CloudTrail to capture all API calls made to the ALB"" is incorrect. CloudTrail captures API activity and would not include the requested information.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 49

A Solutions Architect needs to run a PowerShell script on a fleet of Amazon EC2 instances running Microsoft Windows. The instances have already been launched in an Amazon VPC. What tool can be run from the AWS Management Console that to execute the script on all target EC2 instances?

1. AWS CodeDeploy
2. AWS Config
3. Run Command
4. AWS OpsWorks

Answer: 3

Explanation:

Run Command is designed to support a wide range of enterprise scenarios including installing software, running ad hoc scripts or Microsoft PowerShell commands, configuring Windows Update settings, and more.

Run Command can be used to implement configuration changes across Windows instances on a consistent yet ad hoc basis and is accessible from the AWS Management Console, the AWS Command Line Interface (CLI), the AWS Tools for Windows PowerShell, and the AWS SDKs.

CORRECT: "Run Command" is the correct answer.

INCORRECT: "AWS CodeDeploy" is incorrect. AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services.

INCORRECT: "AWS Config" is incorrect. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It is not used for ad-hoc script execution.

INCORRECT: "AWS OpsWorks" is incorrect. AWS OpsWorks provides instances of managed Puppet and Chef.

References:

<https://aws.amazon.com/blogs/aws/new-ec2-run-command-remote-instance-management-at-scale/>

QUESTION 50

A company requires an Elastic Load Balancer (ELB) for an application they are planning to deploy on AWS. The application requires extremely high throughput and extremely low latencies. The connections will be made using the TCP protocol and the ELB must support load balancing to multiple ports on an instance. Which ELB would should the company use?

1. Classic Load Balancer
2. Application Load Balancer
3. Network Load Balancer
4. Route 53

Answer: 3

Explanation:

The Network Load Balancer operates at the connection level (Layer 4), routing connections to targets – Amazon EC2 instances, containers and IP addresses based on IP protocol data. It is architected to handle millions of requests/sec, sudden volatile traffic patterns and provides extremely low latencies.

The NLB provides high throughput and extremely low latencies and is designed to handle traffic as it grows and can load balance millions of requests/second. NLB also supports load balancing to multiple ports on an instance.

CORRECT: "Network Load Balancer" is the correct answer.

INCORRECT: "Classic Load Balancer" is incorrect. The CLB operates using the TCP, SSL, HTTP and HTTPS protocols. It is not the best choice for requirements of extremely high throughput and low latency and does not support load balancing to multiple ports on an instance.

INCORRECT: "Application Load Balancer" is incorrect. The ALB operates at the HTTP and HTTPS level only (does not support TCP load balancing).

INCORRECT: "Route 53" is incorrect. Route 53 is a DNS service, it is not a type of ELB (though you can do some types of load balancing with it).

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 51

A web application runs on a series of Amazon EC2 instances behind an Application Load Balancer (ALB). A Solutions Architect is updating the configuration with a health check and needs to select the protocol to use. What options are available? (Select TWO.)

1. HTTP
2. SSL
3. HTTPS
4. TCP
5. ICMP

Answer: 1,3

Explanation:

An Application Load Balancer periodically sends requests to its registered targets to test their status. These tests are

called *health checks*.

Each load balancer node routes requests only to the healthy targets in the enabled Availability Zones for the load balancer. Each load balancer node checks the health of each target, using the health check settings for the target groups with which the target is registered. After your target is registered, it must pass one health check to be considered healthy. After each health check is completed, the load balancer node closes the connection that was established for the health check.

If a target group contains only unhealthy registered targets, the load balancer nodes route requests across its unhealthy targets.

For an ALB the possible protocols are HTTP and HTTPS. The default is the HTTP protocol.

CORRECT: "HTTP" is the correct answer.

CORRECT: "HTTPS" is the correct answer.

INCORRECT: "SSL" is incorrect as this is not supported by the ALB.

INCORRECT: "TCP" is incorrect as this is not supported by the ALB.

INCORRECT: "ICMP" is incorrect as this is not supported by the ALB.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 52

A Solutions Architect is designing the disk configuration for an Amazon EC2 instance. The instance needs to support a MapReduce process that requires high throughput for a large dataset with large I/O sizes.

Which Amazon EBS volume is the MOST cost-effective solution for these requirements?

1. EBS General Purpose SSD in a RAID 1 configuration
2. EBS Throughput Optimized HDD
3. EBS Provisioned IOPS SSD
4. EBS General Purpose SSD

Answer: 2

Explanation:

EBS Throughput Optimized HDD is good for the following use cases (and is the most cost-effective option):

- Frequently accessed, throughput intensive workloads with large datasets and large I/O sizes, such as MapReduce, Kafka, log processing, data warehouse, and ETL workloads

Throughput is measured in MB/s, and includes the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume.

CORRECT: "EBS Throughput Optimized HDD" is the correct answer.

INCORRECT: "EBS General Purpose SSD in a RAID 1 configuration" is incorrect. This is not the best solution for the requirements or the most cost-effective.

INCORRECT: "EBS Provisioned IOPS SSD" is incorrect. SSD disks are more expensive.

INCORRECT: "EBS General Purpose SSD" is incorrect. SSD disks are more expensive.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 53

An Amazon EBS-backed EC2 instance has been launched. A requirement has come up for some high-performance ephemeral storage.

How can a Solutions Architect add a new instance store volume?

1. You must shutdown the instance in order to be able to add the instance store volume
2. You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume
3. You can specify the instance store volumes for your instance only when you launch an instance
4. You can use a block device mapping to specify additional instance store volumes when you launch your instance, or you can attach additional instance store volumes after your instance is running

Answer: 3

Explanation:

You can specify the instance store volumes for your instance only when you launch an instance. You can't attach instance store volumes to an instance after you've launched it.

CORRECT: "You can specify the instance store volumes for your instance only when you launch an instance" is the correct answer.

INCORRECT: "You must shutdown the instance in order to be able to add the instance store volume" is incorrect. You can use a block device mapping to specify additional EBS volumes when you launch your instance, or you can attach additional EBS volumes after your instance is running.

INCORRECT: "You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume" is incorrect. An Elastic Network Adapter has nothing to do with adding instance store volumes.

INCORRECT: "You can use a block device mapping to specify additional instance store volumes when you launch your instance, or you can attach additional instance store volumes after your instance is running" is incorrect. You can't attach instance store volumes to an instance after you've launched it.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/add-instance-store-volumes.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 54

A large quantity of data that is rarely accessed is being archived onto Amazon Glacier. Your CIO wants to understand the resilience of the service. Which of the statements below is correct about Amazon Glacier storage? (Select TWO.)

1. Data is replicated globally
2. Provides 99.99999999% durability of archives
3. Data is resilient in the event of one entire Availability Zone destruction
4. Data is resilient in the event of one entire region destruction
5. Provides 99.9% availability of archives

Answer: 2,3

Explanation:

Glacier is designed for durability of 99.99999999% of objects across multiple Availability Zones. Data is resilient in the event of one entire Availability Zone destruction. Glacier supports SSL for data in transit and encryption of data at rest. Glacier is extremely low cost and is ideal for long-term archival.

CORRECT: "Provides 99.99999999% durability of archives" is the correct answer.

CORRECT: "Data is resilient in the event of one entire Availability Zone destruction" is the correct answer.

INCORRECT: "Data is replicated globally" is incorrect. Data is not replicated globally.

INCORRECT: "Data is resilient in the event of one entire region destruction" is incorrect. Data is not resilient to the failure of an entire region.

INCORRECT: "Provides 99.9% availability of archives" is incorrect. Glacier is "designed for" availability of **99.99%**

References:

<https://aws.amazon.com/s3/storage-classes/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/>

QUESTION 55

A Solutions Architect is launching an Amazon EC2 instance with multiple attached volumes by modifying the block device mapping. Which block device can be specified in a block device mapping to be used with an EC2 instance? (Select TWO.)

1. EBS volume
2. EFS volume
3. Instance store volume
4. Snapshot
5. S3 bucket

Answer: 1,3

Explanation:

Each instance that you launch has an associated root device volume, either an Amazon EBS volume or an instance store volume. You can use block device mapping to specify additional EBS volumes or instance store volumes to attach to an instance when it's launched. You can also attach additional EBS volumes to a running instance.

You cannot use a block device mapping to specify a snapshot, EFS volume or S3 bucket.

CORRECT: "EBS volume" is a correct answer.

CORRECT: "Instance store volume" is also a correct answer.

INCORRECT: "EFS volume" is incorrect as described above.

INCORRECT: "Snapshot" is incorrect as described above.

INCORRECT: "S3 bucket" is incorrect as described above.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 56

An Amazon EC2 instance behind an Elastic Load Balancer (ELB) is in the process of being de-registered. Which ELB feature is used to allow existing connections to close cleanly?

1. Sticky Sessions
2. Proxy Protocol
3. Deletion Protection
4. Connection Draining

Answer: 4

Explanation:

Connection draining is enabled by default and provides a period of time for existing connections to close cleanly. When connection draining is in action an CLB will be in the status "InService: Instance deregistration currently in progress".

CORRECT: "Connection Draining" is the correct answer.

INCORRECT: "Sticky Sessions" is incorrect. Session stickiness uses cookies and ensures a client is bound to an individual back-end instance for the duration of the cookie lifetime.

INCORRECT: "Proxy Protocol" is incorrect. The Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connections.

INCORRECT: "Deletion Protection" is incorrect. Deletion protection is used to protect the ELB from deletion.

References:

<https://aws.amazon.com/about-aws/whats-new/2014/03/20/elastic-load-balancing-supports-connection-draining/>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/>

QUESTION 57

The load on a MySQL database running on Amazon EC2 is increasing and performance has been impacted. Which of the options below would help to increase storage performance? (Select TWO.)

1. Use a larger instance size within the instance family
2. Use HDD, Cold (SC1) EBS volumes
3. Use Provisioned IOPS (I01) EBS volumes
4. Use EBS optimized instances
5. Create a RAID 1 array from multiple EBS volumes

Answer: 3,4

Explanation:

EBS optimized instances provide dedicated capacity for Amazon EBS I/O. EBS optimized instances are designed for use with all EBS volume types.

Provisioned IOPS EBS volumes allow you to specify the amount of IOPS you require up to 50 IOPS per GB. Within this limitation you can therefore choose to select the IOPS required to improve the performance of your volume.

RAID can be used to increase IOPS, however RAID 1 does not. For example:

- RAID 0 = 0 striping – data is written across multiple disks and increases performance but no redundancy.
- RAID 1 = 1 mirroring – creates 2 copies of the data but does not increase performance, only redundancy.

HDD, Cold – (SC1) provides the lowest cost storage and low performance

CORRECT: "Use Provisioned IOPS (I01) EBS volumes" is a correct answer.

CORRECT: "Use EBS optimized instances" is also a correct answer.

INCORRECT: "Use a larger instance size within the instance family" is incorrect as this may not increase storage performance.

INCORRECT: "Use HDD, Cold (SC1) EBS volumes" is incorrect. As this will likely decrease storage performance.

INCORRECT: "Create a RAID 1 array from multiple EBS volumes" is incorrect. As explained above, mirroring does not increase performance.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 58

An application receives a high traffic load between 7:30am and 9:30am daily. The application uses an Auto Scaling group to maintain three instances most of the time but during the peak period it requires six instances.

How can a Solutions Architect configure Auto Scaling to perform a daily scale-out event at 7:30am and a scale-in event at 9:30am to account for the peak load?

1. Use a Simple scaling policy
2. Use a Scheduled scaling policy
3. Use a Dynamic scaling policy
4. Use a Step scaling policy

Answer: 2

Explanation:

The following scaling policy options are available:

Simple – maintains a current number of instances, you can manually change the ASGs min/desired/max and attach/detach instances.

Scheduled – Used for predictable load changes, can be a single event or a recurring schedule

Dynamic (event based) – scale in response to an event/alarm.

Step – configure multiple scaling steps in response to multiple alarms.

CORRECT: "Use a Scheduled scaling policy" is the correct answer.

INCORRECT: "Use a Simple scaling policy" is incorrect. Please refer to the description above.

INCORRECT: "Use a Dynamic scaling policy" is incorrect. Please refer to the description above.

INCORRECT: "Use a Step scaling policy" is incorrect. Please refer to the description above.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/>

QUESTION 59

An on-premise data center will be connected to an Amazon VPC by a hardware VPN that has public and VPN-only subnets. The security team has requested that traffic hitting public subnets on AWS that's destined to on-premise applications must be directed over the VPN to the corporate firewall.

How can this be achieved?

1. In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway
2. In the public subnet route table, add a route for your remote network and specify the customer gateway as the target
3. Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway
4. In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target

Answer: 4

Explanation:

Route tables determine where network traffic is directed. In your route table, you must add a route for your remote network and specify the virtual private gateway as the target. This enables traffic from your VPC that's destined for your remote network to route via the virtual private gateway and over one of the VPN tunnels. You can enable route propagation for your route table to automatically propagate your network routes to the table for you.

CORRECT: "In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target" is the correct answer.

INCORRECT: "In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway" is incorrect. You must create the route table rule in the route table attached to the public subnet, not the VPN-only subnet.

INCORRECT: "In the public subnet route table, add a route for your remote network and specify the customer gateway as the target" is incorrect. You must select the virtual private gateway (AWS side of the VPN) not the customer gateway (customer side of the VPN) in the target in the route table.

INCORRECT: "Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway" is incorrect. NAT Gateways are used to enable Internet access for EC2 instances in private subnets, they cannot be used to direct traffic to VPG.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_VPN.html

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario3.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 60

An Amazon DynamoDB table has a variable load, ranging from sustained heavy usage some days, to only having small spikes on others. The load is 80% read and 20% write. The provisioned throughput capacity has been configured to account for the heavy

load to ensure throttling does not occur.

What would be the most efficient solution to optimize cost?

1. Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput
2. Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput
3. Use DynamoDB DAX to increase the performance of the database
4. Create a DynamoDB Auto Scaling scaling policy

Answer: 4

Explanation:

Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This is the most efficient and cost-effective solution to optimizing for cost.

CORRECT: "Create a DynamoDB Auto Scaling scaling policy" is the correct answer.

INCORRECT: "Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput" is incorrect. Using AWS Lambda to modify the provisioned throughput is possible but it would be more cost-effective to use DynamoDB Auto Scaling as there is no cost to using it.

INCORRECT: "Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput" is incorrect. Manually adjusting the provisioned throughput is not efficient.

INCORRECT: "Use DynamoDB DAX to increase the performance of the database" is incorrect. DynamoDB DAX is an in-memory cache that increases the performance of DynamoDB. However, it costs money and there is no requirement to increase performance.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>

QUESTION 61

A Solutions Architect has created a VPC and is in the process of formulating the subnet design. The VPC will be used to host a two-tier application that will include Internet facing web servers, and internal-only DB servers. Zonal redundancy is required.

How many subnets are required to support this requirement?

1. 2 subnets
2. 6 subnets
3. 1 subnet
4. 4 subnets

Answer: 4

Explanation:

Zonal redundancy indicates that the architecture should be split across multiple Availability Zones. Subnets are mapped 1:1 to AZs.

A public subnet should be used for the Internet-facing web servers and a separate private subnet should be used for the internal-only DB servers. Therefore you need 4 subnets – 2 (for redundancy) per public/private subnet.

CORRECT: "4 subnets" is the correct answer.

INCORRECT: "2 subnets" is incorrect as explained above.

INCORRECT: "6 subnets" is incorrect as explained above.

INCORRECT: "2 subnet" is incorrect as explained above.

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 62

The application development team in a company have developed a Java application and saved the source code in a .war file. They would like to run the application on AWS resources and are looking for a service that can handle the provisioning and management of the underlying resources it will run on.

Which AWS service should a Solutions Architect recommend the Developers use to upload the Java source code file?

1. AWS Elastic Beanstalk
2. AWS CodeDeploy
3. AWS CloudFormation
4. AWS OpsWorks

Answer: 1

Explanation:

AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring

Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby, as well as different platform configurations for each language. To use Elastic Beanstalk, you create an application, upload an application version in the form of an application source bundle (for example, a Java .war file) to Elastic Beanstalk, and then provide some information about the application.

CORRECT: "AWS Elastic Beanstalk" is the correct answer.

INCORRECT: "AWS CodeDeploy" is incorrect. AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services.

INCORRECT: "AWS CloudFormation" is incorrect. AWS CloudFormation uses templates to deploy infrastructure as code. It is not a PaaS service like Elastic Beanstalk and is more focused on infrastructure than applications and management of applications.

INCORRECT: "AWS OpsWorks" is incorrect. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.

References:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/>

QUESTION 63

A Solutions Architect has created a new security group in an Amazon VPC. No rules have been created. Which of the statements below are correct regarding the default state of the security group? (Select TWO.)

1. There is an outbound rule that allows all traffic to all IP addresses
2. There are no inbound rules and traffic will be implicitly denied
3. There is an inbound rule allowing traffic from the Internet to port 22 for management
4. There is an inbound rule that allows traffic from the Internet Gateway
5. There is an outbound rule allowing traffic to the Internet Gateway

Answer: 1,2

Explanation:

Custom security groups do not have inbound allow rules (all inbound traffic is denied by default) whereas default security groups do have inbound allow rules (allowing traffic from within the group). All outbound traffic is allowed by default in both custom and default security groups.

Security groups act like a stateful firewall at the instance level. Specifically security groups operate at the network interface level of an EC2 instance. You can only assign permit rules in a security group, you cannot assign deny rules and there is an implicit deny rule at the end of the security group. All rules are evaluated until a permit is encountered or continues until the implicit deny. You can create ingress and egress rules.

CORRECT: "There is an outbound rule that allows all traffic to all IP addresses" is the correct answer.

CORRECT: "There are no inbound rules and traffic will be implicitly denied" is the correct answer.

INCORRECT: "There is an inbound rule allowing traffic from the Internet to port 22 for management" is incorrect. This is not true.

INCORRECT: "There are is an inbound rule that allows traffic from the Internet Gateway" is incorrect. There are no inbound allow rules by default.

INCORRECT: "There is an outbound rule allowing traffic to the Internet Gateway" is incorrect. There is an outbound allow rule but it allows traffic to anywhere, it does not specify the internet gateway.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/>

QUESTION 64

A security officer has requested that all data associated with a specific customer is encrypted. The data resides on Elastic Block Store (EBS) volumes. Which of the following statements about using EBS encryption are correct? (Select TWO.)

1. Not all EBS types support encryption
2. All attached EBS volumes must share the same encryption state
3. All instance types support encryption
4. Data in transit between an instance and an encrypted volume is also encrypted
5. There is no direct way to change the encryption state of a volume

Answer: 4,5

Explanation:

All EBS types and all instance *families* support encryption but not all instance *types* support encryption. There is no direct way to change the encryption state of a volume. Data in transit between an instance and an encrypted volume is also encrypted.

CORRECT: "Data in transit between an instance and an encrypted volume is also encrypted" is the correct answer.

CORRECT: "There is no direct way to change the encryption state of a volume" is the correct answer.

INCORRECT: "Not all EBS types support encryption" is incorrect as all EBS volume types support encryption.

INCORRECT: "All attached EBS volumes must share the same encryption state" is incorrect. You can have encrypted and non-encrypted EBS volumes on a single instance.

INCORRECT: "All instance types support encryption" is incorrect. All instance families support encryption, but not all instance types.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

Save time with our exam-specific cheat sheets:

<https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

QUESTION 65

An organization in the agriculture sector is deploying sensors and smart devices around factory plants and fields. The devices will collect information and send it to cloud applications running on AWS.

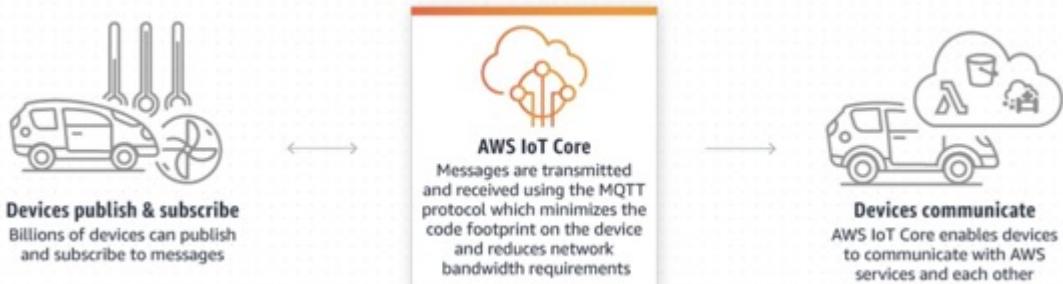
Which AWS service will securely connect the devices to the cloud applications?

1. AWS Glue
2. AWS IoT Core
3. AWS DMS
4. AWS Lambda

Answer: 2

Explanation:

AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely.



CORRECT: "AWS IoT Core" is the correct answer.

INCORRECT: "AWS Glue" is incorrect. AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.

INCORRECT: "AWS DMS" is incorrect. AWS Database Migration Service helps you migrate databases to AWS quickly and securely.

INCORRECT: "AWS Lambda" is incorrect. AWS Lambda lets you run code without provisioning or managing servers.

References:

<https://aws.amazon.com/iot-core/>

CONCLUSION

Congratulations on completing these exam-difficulty practice tests! We truly hope that these high-quality questions along with the supporting explanations helped to fully prepare you for the AWS Certified Solutions Architect Associate exam.

The SAA-C03 exam covers a broad set of technologies and it's vital to ensure you are armed with the knowledge to answer whatever questions come up in your certification exam. So, it's best to review these practice questions until you're confident in all areas. We recommend re-taking these practice tests until you consistently score 80% or higher - that's when you're ready to sit the exam and achieve a great score!

REACH OUT AND CONNECT

We want you to have a 5-star learning experience. If anything is not 100% to your liking, please email us at support@digitalcloud.training. We promise to address all questions and concerns. We really want you to get great value from these training resources.

The AWS platform is evolving quickly, and the exam tracks these changes with a typical lag of around 6 months. We are therefore reliant on student feedback to keep track of what is appearing in the exam. If there are any topics in your exam that weren't covered in our training resources, please provide us with feedback using this form <https://digitalcloud.training/student-feedback/>. We appreciate any feedback that will help us further improve our AWS training resources.

Also, remember to join our private Facebook group to ask questions and share knowledge and exam tips with the AWS community: <https://www.facebook.com/groups/awscertificationqa>

Best wishes for your AWS certification journey!

LIVE BOOTCAMPS, ON-DEMAND TRAINING AND CHALLENGE LABS

At Digital Cloud Training, we offer a wide range of training courses that help students successfully prepare for their AWS certification exams and beyond. Check out our range of training options below.

LIVE BOOTCAMPS (VIRTUAL CLASSROOM)

Our Cloud Mastery Bootcamp is designed to equip learners with job-ready skills that will transform their cloud career. This immersive program includes live hands-on training in a virtual classroom, with a focus on real-world projects and practical skills development.

Our experienced instructors, who possess in-depth industry knowledge, guide our students every step of the way, preparing them for industry-recognized AWS certifications.

The program covers key technologies such as AWS, Python, Linux, Kubernetes, and Terraform, spanning from fundamental cloud concepts to advanced topics.

With no specific prerequisites, anyone can embark on a journey towards a rewarding cloud career. This program opens doors to highly paid cloud roles, incl. Cloud Engineer, DevOps Engineer, or Solutions Architect.

Get ready for your next cloud job with the Cloud Mastery Bootcamp from Digital Cloud Training:

<https://digitalcloud.training/cloud-mastery-bootcamp/>

ON-DEMAND / SELF-PACED AWS TRAINING

Prepare for your next AWS certification with video courses and practice exams. We also offer training notes and practice tests in PDF format for offline study. All of our on-demand training courses are available on digitalcloud.training/aws-training-courses

Gain unlimited access to ALL of our on-demand courses – current and future – with early access to new content and updates. To get a taste, start your monthly plan or sign up for 12 months of unlimited access to our entire library of cloud training courses.

To learn more, visit <https://digitalcloud.training/all-access/>

CHALLENGE LABS

Keen to gain practical, real-world cloud skills? Then Challenge Labs are for you. Hone your skills across the most in-demand technologies, practice role-based cloud skills, and get the hands-on experience you need for certification exams.

Hands-on Challenge Labs are scenario-based exercises that run in a secure sandbox environment. These online scored labs offer extensive hands-on opportunities for all skill levels without the risk of running up any cloud bills!

Ranging from fully guided to advanced hands-on exercises, Challenge Labs cater for all skill levels. At Digital Cloud Training we offer Challenge Labs for different levels of learners:

- **Guided** – Simply follow the step-by-step instructions in the guided labs with detailed hints to learn the fundamentals.
- **Advanced** – Create solutions according to requirements with supporting documentation – each step is checked and validated.
- **Expert** – Create solutions according to requirements with basic instructions and no supporting information and receive a final score.

Our Challenge Labs catalog includes over 1000 on-demand challenges across multiple cloud platforms and technologies including AWS, Azure, Docker, Linux, Microsoft, VMware and Cybersecurity.

To learn more, visit <https://digitalcloud.training/hands-on-challenge-labs/>

ABOUT THE AUTHOR



Neal Davis is the founder of [Digital Cloud Training](#), AWS Cloud Solutions Architect and successful IT instructor. With more than two decades of experience in the Cloud Computing industry, Neal is a true expert in solutions architecture. In 2018, he founded [Digital Cloud Training](#) with the primary goal of bringing the highest quality AWS certification training resources to the market. His passion for teaching technology is matched by his commitment to helping his students achieve their cloud career goals.

Digital Cloud Training offers top-quality training resources to help students thrive in the cloud computing industry – including [live bootcamps](#), [on-demand video courses](#) and [hands-on Challenge Labs](#) - designed to equip learners with job-ready skills.

With Digital Cloud Training, you get access to highly experienced instructors who support you on your cloud journey and help you elevate your career through achieving highly valuable certifications and developing real-world experience. Join the AWS Community of over 750,000 happy students that enrolled in Digital Cloud Training courses.

CONNECT WITH US ON SOCIAL MEDIA

All Links available on <https://digitalcloud.training/about-neal-davis-and-digital-cloud-training/>



digitalcloud.training



facebook.com/digitalcloudtraining



linkedin.com/company/digitalcloudtraining



youtube.com/c/digitalcloudtraining



Twitter @[digitalcloudt](#)



Instagram @[digitalcloudtraining](#)