Answer Sheet

Q1)

You are looking for a method to distribute onboarding videos to your company痴 numerous remote workers around the world. The training videos are located in an S3 bucket that is not publicly accessible.

Which of the options below would allow you to share the videos?

- Use ElastiCache and attach the S3 bucket as a cache origin
- ✅ Use CloudFront and set the S3 bucket as an origin

Explanation:-CloudFront uses origins which specify 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). When using Amazon S3 as an origin you place all of your objects within the bucket You cannot configure an origin with ElastiCache You cannot use a Route 53 Alias record to connect to an S3 bucket that is not publicly available You can configure a custom origin pointing to an EC2 instance but as the training videos are located in an S3 bucket this would not be helpful. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

- Use a Route 53 Alias record the points to the S3 bucket
- Use CloudFront and use a custom origin pointing to an EC2 instance

---

Q2)

Your company runs a two-tier application that uses web front-ends running on EC2 instances across multiple AZs. The back-end is an RDS multi-AZ database instance. The front-end servers host a Content Management System (CMS) application that stores files that users upload in attached EBS storage. You don稚 like having the uploaded files distributed across multiple EBS volumes and are concerned that this solution is not scalable.

You would like to design a solution for storing the files that are uploaded to your EC2 instances that can achieve high levels of aggregate throughput and IOPS. The solution must scale automatically, and provide consistent low latencies. You also need to be able to mount the storage to the EC2 instances across multiple AZs within the region.

Which AWS service would meet your needs?

- ✅ Use the Amazon Elastic File System

Explanation:-The Amazon Elastic File System (EFS) is a file-based (not block or object-based) system that is accessed using the NFSv4.1 protocol. You can concurrently connect 1 to 1000s of EC2 instances from multiple AZs to a single EFS file system. EFS is elastic and provides high levels of aggregate throughput and IOPS. Amazon S3 is an object-based solution and cannot be mounted to EC2 instances ElastiCache is an in-memory database used for caching data and providing high performance access, it it not a file storage solution that can be mounted to EC2 instances RDS is a relational database and cannot be mounted to EC2 instances and used to store files. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

- Use ElastiCache
- Store the files in the RDS database
- Create an S3 bucket and use this as the storage location for the application

---

Q3)

You work as a Solutions Architect at Digital Cloud Training. You are working on a disaster recovery solution that allows you to bring up your applications in another AWS region. Some of your applications run on EC2 instances and have proprietary software configurations with embedded licenses. You need to create duplicate copies of your EC2 instances in the other region.

What would be the best way to do this? (choose 2)

- ✅ Create an AMI of each EC2 instance and copy the AMIs to the other region

Explanation:-In this scenario we are not looking to backup the instances but to create identical copies of them in the other region. These are often called golden images. We must assume that any data used by the instances resides in another service and will be accessible to them when they are launched in a DR situation You launch EC2 instances using AMIs not snapshots (you can create AMIs from snapshots). Therefore, you should create AMIs of each instance (rather than snapshots), copy the AMIs between regions and then create new EC2 instances from the AMIs AMIs are regional as they are backed by Amazon S3. You can only launch an AMI from the region in which it is stored. However, you can copy AMI痴 to other regions using the console, command line, or the API References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

- ✅ Create new EC2 instances from the AMIs

Explanation:-In this scenario we are not looking to backup the instances but to create identical copies of them in the other region. These are often called golden images. We must assume that any data used by the instances resides in another service and will be accessible to them when they are launched in a DR situation You launch EC2 instances using AMIs not snapshots (you can create AMIs from snapshots). Therefore, you should create AMIs of each instance (rather than snapshots), copy the AMIs between regions and then create new EC2 instances from the AMIs AMIs are regional as they are backed by Amazon S3. You can only launch an AMI from the region in which it is stored. However, you can copy AMI痴 to other regions using the console, command line, or the API. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

- Copy the snapshots to the other region
- Create snapshots of the EBS volumes attached to the instances

---

Q4) A Solutions Architect requires a highly available database that can deliver an extremely low RPO. Which of the following configurations uses synchronous replication?

- EBS volume synchronization
- ✅ RDS DB instance using a Multi-AZ configuration

Explanation:-A Recovery Point Objective (RPO) relates to the amount of data loss that can be allowed, in this case a low RPO means that you need to minimize the amount of data lost so synchronous replication is required. Out of the options presented only Amazon RDS in a multi-AZ configuration uses synchronous replication RDS Read Replicas use asynchronous replication and are not used for DR DynamoDB Read Replicas

do not exist EBS volume synchronization does not exist. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- RDS Read Replica across AWS regions
- DynamoDB Read Replica

Q5) You have taken a snapshot of an encrypted EBS volume and would like to share the snapshot with another AWS account. Which statements are true about sharing snapshots of encrypted EBS volumes? (choose 2)

- Snapshots of encrypted volumes are unencrypted
- ✅ A custom CMK key must be used for encryption if you want to share the snapshot

Explanation:-A custom CMK key must be used for encryption if you want to share the snapshot You must share the CMK key as well as the snapshot with the other AWS account Snapshots of encrypted volumes are encrypted automatically To share an encrypted snapshot you must encrypt it in the source account with a custom CMK key and then share the key with the target account You do not need to store the CMK key in CloudHSM References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

- You must store the CMK key in CloudHSM and delegate access to the other AWS account
- ✅ You must share the CMK key as well as the snapshot with the other AWS account

Explanation:-A custom CMK key must be used for encryption if you want to share the snapshot You must share the CMK key as well as the snapshot with the other AWS account Snapshots of encrypted volumes are encrypted automatically To share an encrypted snapshot you must encrypt it in the source account with a custom CMK key and then share the key with the target account You do not need to store the CMK key in CloudHSM. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

Q6)

A company is launching a new application and expects it to be very popular. The company requires a database layer that can scale along with the application. The schema will be frequently changes and the application cannot afford any downtime for database changes.

Which AWS service allows the company to achieve these requirements?

- ✅ Amazon DynamoDB

Explanation:-DynamoDB a NoSQL DB which means you can change the schema easily. It's also the only DB in the list that you can scale without any downtime Amazon Aurora, RDS MySQL and RedShift all require changing instance sizes in order to scale which causes an outage. They are also all relational databases (SQL) so changing the schema is difficult References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

- Amazon RDS MySQL
- Amazon Aurora
- Amazon RedShift

Q7)

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The web servers must be accessible only to customers on an SSL connection. The database should only be accessible to web servers in a public subnet.

Which solution meets these requirements without impacting other running applications? (choose 2)

- ✅ Create a web server security group that allows HTTPS port 443 inbound traffic from Anywhere (0.0.0.0/0) and apply it to the web servers

Explanation:-A VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic. Custom network ACLs deny everything inbound and outbound by default but in this case a default network ACL is being used Inbound connections to web servers will be coming in on port 443 from the Internet so creating a security group to allow this port from 0.0.0.0/0 and applying it to the web servers will allow this traffic The MySQL DB will be listening on port 3306. Therefore, the security group that is applied to the DB servers should allow 3306 inbound from the web servers security group The DB server is listening on 3306 so creating a rule allowing 443 inbound will not help References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Create a network ACL on the DB subnet, allow MySQL port 3306 inbound for web servers, and deny all outbound traffic
- Create a network ACL on the web server's subnet, allow HTTPS port 443 inbound, and specify the source as 0.0.0.0/0
- ✅ Create a DB server security group that allows MySQL port 3306 inbound and specify the source as a web server security group

Explanation:-A VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic. Custom network ACLs deny everything inbound and outbound by default but in this case a default network ACL is being used Inbound connections to web servers will be coming in on port 443 from the Internet so creating a security group to allow this port from 0.0.0.0/0 and applying it to the web servers will allow this traffic The MySQL DB will be listening on port 3306. Therefore, the security group that is applied to the DB servers should allow 3306 inbound from the web servers security group The DB server is listening on 3306 so creating a rule allowing 443 inbound will not help References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q8) You are considering the security and durability of your data that is stored in Amazon EBS volumes. Which of the statements below is true?

- You can define the number of AZs to replicate your data to via the API
- EBS volumes are backed by Amazon S3 which replicates data across multiple facilities within a region
- EBS volumes are replicated across AZs to protect you from loss of access to an individual AZ
- ✅ EBS volumes are replicated within their Availability Zone (AZ) to protect you from component failure

Explanation:-EBS volume data is replicated across multiple servers within an AZ EBS volumes are not replicated across AZs EBS volumes are not automatically backed up to Amazon S3 so there is no durability here. However, snapshots of EBS volumes do reside on S3 There is no option to define the number of AZs you can replicate your data. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

Q9)

Your company is opening a new office in the Asia Pacific region. Users in the new office will need to read data from an RDS database that is hosted in the U.S. To improve performance, you are planning to implement a Read Replica of the database in

the Asia Pacific region. However, your Chief Security Officer (CSO) has explained to you that the company policy dictates that all data that leaves the U.S must be encrypted at rest. The master RDS DB is not currently encrypted.

What options are available to you? (choose 2)

✅ You can create an encrypted Read Replica that is encrypted with a different key

Explanation:-You cannot encrypt an existing DB, you need to create a snapshot, copy it, encrypt the copy, then build an encrypted DB from the snapshot You can encrypt your Amazon RDS instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instance Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots A Read Replica of an Amazon RDS encrypted instance is also encrypted using the same key as the master instance when both are in the same region If the master and Read Replica are in different regions, you encrypt using the encryption key for that region You can't have an encrypted Read Replica of an unencrypted DB instance or an unencrypted Read Replica of an encrypted DB instance. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

⚪ You can create an encrypted Read Replica that is encrypted with the same key

✅ You can enable encryption for the master DB by creating a new DB from a snapshot with encryption enabled

Explanation:-You cannot encrypt an existing DB, you need to create a snapshot, copy it, encrypt the copy, then build an encrypted DB from the snapshot You can encrypt your Amazon RDS instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instance Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots A Read Replica of an Amazon RDS encrypted instance is also encrypted using the same key as the master instance when both are in the same region If the master and Read Replica are in different regions, you encrypt using the encryption key for that region You can't have an encrypted Read Replica of an unencrypted DB instance or an unencrypted Read Replica of an encrypted DB instance. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

⚪ You can enable encryption for the master DB through the management console

---

Q10) A company is planning moving their DNS records to AWS as part of a major migration to the cloud. Which statements are true about Amazon Route 53? (choose 2)

✅ You cannot automatically register EC2 instances with private hosted zones

Explanation:-You cannot automatically register EC2 instances with private hosted zones Route 53 can be used to route Internet traffic for domains registered with another domain registrar (any domain) You can transfer domains to Route 53 only if the Top Level Domain (TLD) is supported. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

⚪ You can automatically register EC2 instances with private hosted zones

⚪ You can transfer domains to Route 53 even if the Top-Level Domain (TLD) is unsupported

✅ Route 53 can be used to route Internet traffic for domains registered with another domain registrar

Explanation:-You cannot automatically register EC2 instances with private hosted zones Route 53 can be used to route Internet traffic for domains registered with another domain registrar (any domain) You can transfer domains to Route 53 only if the Top Level Domain (TLD) is supported. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

Q11)

A developer is creating a solution for a real-time bidding application for a large retail company that allows users to bid on items of end-of-season clothing. The application is expected to be extremely popular and the back-end DynamoDB database may not perform as required

How can the Solutions Architect enable in-memory read performance with microsecond response times for the DynamoDB database?

⚪ Enable read replicas

⚪ Increase the provisioned throughput

⚪ Configure DynamoDB Auto Scaling

✅ Configure Amazon DAX

Explanation:-Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement from milliseconds to microseconds even at millions of requests per second. You can enable DAX for a DynamoDB database with a few clicks Provisioned throughput is the maximum amount of capacity that an application can consume from a table or index, it doesn't improve the speed of the database or add in-memory capabilities DynamoDB auto scaling actively manages throughput capacity for tables and global secondary indexes so like provisioned throughput it does not provide the speed or in-memory capabilities requested There is no such thing as read replicas with DynamoDB. References: https://aws.amazon.com/dynamodb/dax/

Q12) You have launched a Spot instance on EC2 for working on an application development project. In the event of an interruption what are the possible behaviors that can be configured? (choose 2)

✅ Hibernate

Explanation:-You can specify whether Amazon EC2 should hibernate, stop, or terminate Spot Instances when they are interrupted. You can choose the interruption behavior that meets your needs. The default is to terminate Spot Instances when they are interrupted You cannot configure the interruption behavior to restart, save, or pause the instance. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html

⚪ Restart

✅ Stop

Explanation:-You can specify whether Amazon EC2 should hibernate, stop, or terminate Spot Instances when they are interrupted. You can choose the interruption behavior that meets your needs. The default is to terminate Spot Instances when they are interrupted You cannot configure the interruption behavior to restart, save, or pause the instance. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html

⚪ Pause

Q13) Your company SysOps practices involve running scripts within the Linux operating systems of your applications. Which of the following AWS services allow you to access the underlying operating system? (choose 2)

✅ Amazon EC2

Explanation:-You can access Amazon EMR by using the AWS Management Console, Command Line Tools, SDKs, or the EMR API With EMR and EC2 you have access to the underlying operating system which means you can connect to the operating system using protocols such as SSH and then manage the operating system The other services listed are managed services that do not allow access to the underlying operating systems on which the services run References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

⚪ Amazon RDS

⚪ AWS Lambda

✅ Amazon EMR

Explanation:-You can access Amazon EMR by using the AWS Management Console, Command Line Tools, SDKs, or the EMR API With EMR and EC2 you have access to the underlying operating system which means you can connect to the operating system using protocols such as SSH and then manage the operating system The other services listed are managed services that do not allow access to the underlying operating systems on which the services run References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

Q14)

Another systems administrator in your company created an Auto Scaling group that is configured to ensure that four EC2 instances are available at a minimum at all times. The settings he selected on the Auto Scaling group are a minimum group size of four instances and a maximum group size of six instances.Your colleague has asked your assistance in trying to understand if Auto Scaling will allow him to terminate instances in the Auto Scaling group and what the effect would be if it does.

What advice would you give to your colleague?

⚪ Auto Scaling will not allow him to terminate an EC2 instance, because there are currently four provisioned instances and the minimum is set to four

⚪ This can only be done via the command line

⚪ He would need to reduce the minimum group size setting to be able to terminate any instances

✅ This should be allowed, and Auto Scaling will launch additional instances to compensate for the ones that were terminated

Explanation:-You can terminate instances in the ASG and Auto Scaling will then perform rebalancing when it finds that the number of instances across AZs is not balanced Auto Scaling will not prevent an imbalance from occurring by stopping you from terminating instances, but it will react to the imbalance by attempting to rebalance by launching new instances You do not need to reduce the minimum group size and terminating instances does not need to be performed using the command line References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

Q15)

A company is moving a large amount of sensitive data to the cloud. Data will be moved to Amazon S3 and the Solutions Architects are concerned about encryption and management of keys.

Which of the statements below is correct regarding the SSE-KMS option? (choose 2)

✅ Auditable master keys can be created, rotated, and disabled from the IAM console

Explanation:-You can use server-side encryption with SSE-KMS to protect your data with a master key or you can use an AWS KMS customer master key KMS uses customer master keys (CMKs), not customer provided keys SSE-KMS requires that AWS manage the data key but you manage the master key in AWS KMS Auditable master keys can be created, rotated, and disabled from the IAM console You can use the Amazon S3 encryption client in the AWS SDK from your own application to encrypt objects and upload them to Amazon S3, otherwise data is encrypted on Amazon S3, not on the client side References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

✅ KMS uses customer master keys (CMKs)

Explanation:-You can use server-side encryption with SSE-KMS to protect your data with a master key or you can use an AWS KMS customer master key KMS uses customer master keys (CMKs), not customer provided keys SSE-KMS requires that AWS manage the data key but you manage the master key in AWS KMS Auditable master keys can be created, rotated, and disabled from the IAM console You can use the Amazon S3 encryption client in the AWS SDK from your own application to encrypt objects and upload them to Amazon S3, otherwise data is encrypted on Amazon S3, not on the client side References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

⚪ KMS uses customer provided keys (CPKs)

⚪ Keys are managed through Amazon S3

Q16)

A colleague recently deployed a two-tier web application into a subnet using a test account. The subnet has an IP address block of 10.0.5.0/27 and he launched an Auto Scaling Group (ASG) with a desired capacity of 8 web servers. Another ASG has 6 application servers and two database servers and both ASGs are behind a single ALB with multiple target groups. All instances are On-Demand instances. Your colleague attempted to test a simulated increase in capacity requirements of 50% and not all instances were able to launch successfully.

What would be the best explanations for the failure to launch the extra instances? (choose 2)

⚪ There are insufficient resources available in the Availability Zone

✅ AWS impose a soft limit of 20 instances per region for an account, you have exceeded this number

Explanation:-The relevant facts are there is a soft limit of 20 On-demand or 20 reserved instances per region by default and there are 32 possible hosts in a /27 subnet. AWS reserve the first 4 and last 1 IP address. ELB requires 8 addresses within your subnet which only leaves 19 addresses available for use There are 16 EC2 instances so a capacity increase of 50% would bring the total up to 24 instances which exceeds the address space and the default account limit for On-Demand instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

✅ There are insufficient IP addresses in the subnet range to allow for the EC2 instances, the AWS reserved addresses, and the ELB IP address requirements

Explanation:-The relevant facts are there is a soft limit of 20 On-demand or 20 reserved instances per region by default and there are 32 possible hosts in a /27 subnet. AWS reserve the first 4 and last 1 IP address. ELB requires 8 addresses within your subnet which only leaves 19 addresses available for use There are 16 EC2 instances so a capacity increase of 50% would bring the total up to 24 instances which exceeds the address space and the default account limit for On-Demand instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

The IP address block overlaps with another subnet in the VPC

Q17) A Solutions Architect is reviewing the IP addressing strategy for the company's resources in the AWS Cloud. Which of the statements below are correct regarding private IP addresses? (choose 2)

For instances launched in a VPC, a private IPv4 address remains associated with the network interface when the instance is stopped and restarted

Explanation:-For instances launched in EC2-Classic, the private IPv4 address is released when the instance is stopped or terminated For instances launched in a VPC, a private IPv4 address remains associated with the network interface when the instance is stopped and restarted By default an instance only has a single private IP address Secondary private IP addresses can be reassigned from one instance to another (the primary IPs cannot) A private IPv4 address is not reachable over the Internet References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

Secondary private IP addresses cannot be reassigned from one instance to another

For instances launched in EC2-Classic, the private IPv4 address is released when the instance is stopped or terminated

Explanation:-For instances launched in EC2-Classic, the private IPv4 address is released when the instance is stopped or terminated For instances launched in a VPC, a private IPv4 address remains associated with the network interface when the instance is stopped and restarted By default an instance only has a single private IP address Secondary private IP addresses can be reassigned from one instance to another (the primary IPs cannot) A private IPv4 address is not reachable over the Internet References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

A private IPv4 address is an IP address that's reachable over the Internet

---

Q18)

The operations team in your company are looking for a method to automatically respond to failed system status check alarms that are being received from an EC2 instance. The system in question is experiencing intermittent problems with its operating system software.

Which two steps will help you to automate the resolution of the operating system software issues? (choose 2)

Configure an EC2 action that terminates the instance

Create a CloudWatch alarm that monitors the 鉄tatusCheckFailed_Instance?? metric

Explanation:-EC2 status checks are performed every minute and each returns a pass or a fail status. If all checks pass, the overall status of the instance is OK. If one or more checks fail, the overall status is impaired System status checks detect (StatusCheckFailed_System) problems with your instance that require AWS involvement to repair whereas Instance status checks (StatusCheckFailed_Instance) detect problems that require your involvement to repair The action to recover the instance is only supported on specific instance types and can be used only with StatusCheckFailed_System Configuring an action to terminate the instance would not help resolve system software issues as the instance would be terminated References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

Configure an EC2 action that recovers the instance

Configure an EC2 action that reboots the instance

Explanation:-EC2 status checks are performed every minute and each returns a pass or a fail status. If all checks pass, the overall status of the instance is OK. If one or more checks fail, the overall status is impaired System status checks detect (StatusCheckFailed_System) problems with your instance that require AWS involvement to repair whereas Instance status checks (StatusCheckFailed_Instance) detect problems that require your involvement to repair The action to recover the instance is only supported on specific instance types and can be used only with StatusCheckFailed_System Configuring an action to terminate the instance would not help resolve system software issues as the instance would be terminated References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

Q19)

You are using an Application Load Balancer (ALB) for distributing traffic for a number of application servers running on EC2 instances. The configuration consists of a single ALB with a single target group. The front-end listeners are receiving traffic for digitalcloud.guru on port 443 (SSL/TLS) and the back-end listeners are receiving traffic on port 80 (HTTP).You will be installing a new application component on one of the application servers in the existing target group that will process data sent to digitalcloud.guru/orders. The application component will listen on HTTP port 8080 for this traffic.

What configuration changes do you need to make to implement this solution update? (choose 2)

Create a new target group and add the EC2 instance to it. Define the protocol as HTTP and the port as 8080

Explanation:-The traffic is coming in on standard ports (443/HTTPS, 80/HTTP) to a single front-end listener. You can only have a single listener running on a single port. Therefore to be able to direct traffic for a specific web page you need to use an ALB and path-based routing to direct the traffic to a specific back-end listener. As only one protocol and one port can be defined per target group you also need to create a new target group that uses port 8080 as a target. As discussed above you cannot add additional ports to existing target groups as you can only have a single protocol/port per target group Host conditions (host-based routing) route client requests based on the Host field of the HTTP header allowing you to route to multiple domains from the same load balancer - in this case we are not directing traffic based on the host field (digitalcloud.training), which does not change in this scenario, we are directing traffic based on the path field (/orders) You also cannot add an additional front-end listener that listens on the same port as another listener References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Add an additional front-end listener that listens on port 443 and set a path condition to process traffic destined to the path /orders

Add a new rule to the existing front-end listener with a Host condition. Set the host condition to /orders and add an action that forwards traffic to the new target group

Add a new rule to the existing front-end listener with a Path condition. Set the path condition to /orders and add an action that forwards traffic to the new target group

Explanation:-The traffic is coming in on standard ports (443/HTTPS, 80/HTTP) to a single front-end listener. You can only have a single listener running on a single port. Therefore to be able to direct traffic for a specific web page you need to use an ALB and path-based routing to direct the traffic to a specific back-end listener. As only one protocol and one port can be defined per target group you also need to create a new target group that uses port 8080 as a target. As discussed above you cannot add additional ports to existing target groups as you can only have a single protocol/port per target group Host conditions (host-based routing) route client requests based on the Host field of the HTTP header allowing you to route to multiple domains from the same load balancer - in this case we are not directing traffic based on the host field (digitalcloud.training), which does not change in this scenario, we are directing traffic based on the path field (/orders) You also cannot add an additional front-end listener that listens on the same port as another listener References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q20) A client is in the design phase of developing an application that will process orders for their online ticketing system. The application will use a number of front-end EC2 instances that pick-up orders and place them in a queue for processing by another set of back-end EC2 instances. The client will have multiple options for customers to choose the level of service they want to pay for. The client has asked how he can design the application to process the orders in a prioritized way based on the level of service the customer has chosen

- Create multiple SQS queues, configure exactly-once processing and set the maximum visibility timeout to 12 hours
- Create a combination of FIFO queues and Standard queues and configure the applications to place messages into the relevant queue based on priority
- ✅ Create multiple SQS queues, configure the front-end application to place orders onto a specific queue based on the level of service requested and configure the back-end instances to sequentially poll the queues in order of priority

Explanation:-The best option is to create multiple queues and configure the application to place orders onto a specific queue based on the level of service. You then configure the back-end instances to poll these queues in order or priority so they pick up the higher priority jobs first Creating a combination of FIFO and standard queues is incorrect as creating a mixture of queue types is not the best way to separate the messages, and there is nothing in this option that explains how the messages would be picked up in the right order Creating a single queue and configuring the applications to place orders on the queue in order of priority would not work as standard queues offer best-effort ordering so there痴 no guarantee that the messages would be picked up in the correct order Creating multiple SQS queues and configuring exactly-once processing (only possible with FIFO) would not ensure that the order of the messages is prioritized References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/

- Create a single SQS queue, configure the front-end application to place orders on the queue in order of priority and configure the back-end instances to poll the queue and pick up messages in the order they are presented

---

Q21)

There are two business units in your company that each have their own VPC. A company restructure has resulted in the need to work together more closely and you would like to configure VPC peering between the two VPCs. VPC A has a CIDR block of 172.16.0.0/16 and VPC B has a CIDR block of 10.0.0.0/16. You have created a VPC peering connection with the ID: pcx-11112222.

Which of the entries below should be added to the route table to allow full access to the entire CIDR block of the VPC peer? (choose 2)

- Destination 10.0.0.0/16 and target pcx-11112222 in VPC B
- ✅ Destination 10.0.0.0/16 and target pcx-11112222 in VPC A

Explanation:-Please note that though this is an incomplete solution. Sometimes in the exam you'll be offered solutions that are incomplete or for which you have to make assumptions. You'll also sometimes be offered multiple correct responses and have to choose the best or most cost-effective option The full list of route tables entries required for this solution are: - Destination 172.16.0.0/16 and target Local in VPC A - Destination 10.0.0.0/16 and target pcx-11112222 in VPC A - Destination 10.0.0.0/16 and target Local in VPC B - Destination 172.16.0.0/16 and target pcx.11112222 in VPC B Refer to the URL below for more details around this scenario References: https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html

- ✅ Destination 172.16.0.0/16 and target pcx.11112222 in VPC B

Explanation:-Please note that though this is an incomplete solution. Sometimes in the exam you'll be offered solutions that are incomplete or for which you have to make assumptions. You'll also sometimes be offered multiple correct responses and have to choose the best or most cost-effective option The full list of route tables entries required for this solution are: - Destination 172.16.0.0/16 and target Local in VPC A - Destination 10.0.0.0/16 and target pcx-11112222 in VPC A - Destination 10.0.0.0/16 and target Local in VPC B - Destination 172.16.0.0/16 and target pcx.11112222 in VPC B Refer to the URL below for more details around this scenario References: https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html

- Destination 0.0.0.0/0 and target Local in VPC A and VPC B

Q22)

As the Chief Security Officer (CSO) of a large banking organization you are reviewing your security policy for the usage of public cloud services. A key assessment criteria when comparing public cloud services against maintaining applications on-premise, is the split of responsibilities between AWS, as the service provider, and your company, as the customer.

According to the AWS Shared Responsibility Model, which of the following would be responsibilities of the service provider? (choose 2)

- ✅ Physical networking infrastructure

Explanation:-AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services The customer is responsible for security of the resources they provision. Customer responsibilities include operating system, network and firewall configuration, identity and access management, and customer data References: https://aws.amazon.com/compliance/shared-responsibility-model/

- Identity and Access Management
- Operating system, network and firewall configuration
- ✅ Availability Zones

Explanation:-AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services The customer is responsible for security of the resources they provision. Customer responsibilities include operating system, network and firewall configuration, identity and access management, and customer data References: https://aws.amazon.com/compliance/shared-responsibility-model/

Q23)

You are running a Hadoop cluster on EC2 instances in your VPC. The EC2 instances are launched by an Auto Scaling Group (ASG) and you have configured the ASG to scale out and in as demand changes. One of the instances in the group is the Hadoop Master Node and you need to ensure that it is not terminated when your ASG processes a scale in action.

What is the best way this can be achieved without interrupting services?

- Move the Hadoop Master Node to another ASG that has the minimum and maximum instance settings set to 1
- ✅ Use the Instance Protection feature to set scale in protection for the Hadoop Master Node

Explanation:-You can enable Instance Protection to protect a specific instance in an ASG from a scale in action Moving the Hadoop Node to another ASG would work but is impractical and would incur service interruption EC2 has a feature called 鍍ermination protection?? not 泥eletion Protection?? The 泥eleteOnTermination?? value relates to EBS volumes not EC2 instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://aws.amazon.com/blogs/aws/new-instance-protection-for-auto-scaling/

- Enable Deletion Protection for the EC2 instance
- Change the DeleteOnTermination value for the EC2 instance

Q24)

The development team in your company has created a new application that you plan to deploy on AWS which runs multiple components in Docker containers. You would prefer to use AWS managed infrastructure for running the containers as you do not want to manage EC2 instances.

Which of the below solution options would deliver these requirements? (choose 2)

- Put your container images in a private repository
- ✅ Put your container images in the Elastic Container Registry (ECR)

Explanation:-If you do not wand to manage EC2 instances you must use the AWS Fargate launch type which is a serverless infrastructure managed by AWS. Fargate only supports container images hosted on Elastic Container Registry (ECR) or Docker Hub The EC2 Launch Type allows you to run containers on EC2 instances that you manage Private repositories are only supported by the EC2 Launch Type You cannot use CloudFront (a CDN) to deploy Docker on EC2 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

- Use the Elastic Container Service (ECS) with the EC2 Launch Type
- ✅ Use the Elastic Container Service (ECS) with the Fargate Launch Type

Explanation:-If you do not wand to manage EC2 instances you must use the AWS Fargate launch type which is a serverless infrastructure managed by AWS. Fargate only supports container images hosted on Elastic Container Registry (ECR) or Docker Hub The EC2 Launch Type allows you to run containers on EC2 instances that you manage Private repositories are only supported by the EC2 Launch Type You cannot use CloudFront (a CDN) to deploy Docker on EC2 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

Q25)

You are designing a solution for an application that will read and write large amounts of data to S3. You are expecting high throughput that may exceed 1000 requests per second and need the performance of S3 to scale.

What is AWS痴 current advice for designing your S3 storage strategy to ensure fast performance?

- ✅ There is no longer a need to use random prefixes as S3 scales per prefix and the performance required is well within the S3 performance limitations

Explanation:-According to the latest information, AWS no longer require random prefixes as they have improved S3 so that it can scale to higher throughput and per prefix Caution is required as the exam may not yet reflect these changes You do not need to use CloudFront for caching objects because of performance concerns with S3. CloudFront is more for performance concerns where end-users need to access objects over the Internet There is no such thing as an object cache in Amazon S3 References: https://aws.amazon.com/about-aws/whats-new/2018/07/amazon-s3-announces-increased-request-rate-performance/

- You must use CloudFront for caching objects at this scale as S3 cannot provide this level of performance
- Enable an object cache on S3 to ensure performance at this scale
- Use a random prefix on objects to improve performance

Q26)

You are deploying a two-tier web application within your VPC. The application consists of multiple EC2 instances and an Internet-facing Elastic Load Balancer (ELB). The application will be used by a small number of users with fixed public IP addresses and you need to control access so only these users can access the application.

What would be the BEST methods of applying these controls? (choose 2)

- Configure the EC2 instance痴 Security Group to allow traffic from only the specific IP sources
- ✅ Configure the ELB to send the X-Forwarded-For header and configure the EC2 instances to filter traffic based on the source IP information in the header

Explanation:-There are two practical methods of implementing these controls and these can be used in isolation or together (defence in depth). As the clients have fixed IPs you can configure a security group to control access by only permitting these addresses. The ELB security group is the correct place to implement this control. You can also configured ELB to forward the X-Forwarded-For header which means the source IP information is carried through to the EC2 instances. You are then able to configure security controls for the addresses at the EC2 instance level, for instance by using an iptables firewall ELB does not support client certificate authentication (API Gateway does support this) The EC2 instance Security Group is the wrong place to implement the allow rule References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- Configure the local firewall on each EC2 instance to only allow traffic from the specific IP sources
- ✅ Configure the ELB Security Group to allow traffic from only the specific IP sources

Explanation:-There are two practical methods of implementing these controls and these can be used in isolation or together (defence in depth). As the clients have fixed IPs you can configure a security group to control access by only permitting these addresses. The ELB security group is the correct place to implement this control. You can also configured ELB to forward the X-Forwarded-For header which means the source IP information is carried through to the EC2 instances. You are then able to configure security controls for the addresses at the EC2 instance level, for instance by using an iptables firewall ELB does not support client certificate authentication (API Gateway does support this) The EC2 instance Security Group is the wrong place to implement the allow rule References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q27)

A customer has a production application running on Amazon EC2. The application frequently overwrites and deletes data, and it is essential that the application receives the most up-to-date version of the data whenever it is requested.

Which service is most appropriate for these requirements?

- Amazon RedShift
- AWS Storage Gateway
- Amazon S3
- ✅ Amazon RDS

Explanation:-This scenario asks that when retrieving data the chosen storage solution should always return the most up-to-date data. Therefore we must use Amazon RDS as it provides read-after-write consistency Amazon S3 only provides eventual consistency for overwrites and deletes Amazon RedShift is a data warehouse and is not used as a transactional database so this is the wrong use case for it AWS Storage Gateway is used for enabling hybrid cloud access to AWS storage services from on-premises References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

Q28)

A Solutions Architect is developing a new web application on AWS that needs to be able to scale to support unpredictable workloads. The Architect prefers to focus on value-add activities such as software development and product roadmap development rather than provisioning and managing instances.

Which solution is most appropriate for this use case?

- Elastic Load Balancing with Auto Scaling groups and Amazon EC2
- Amazon CloudFront and AWS Lambda
- Amazon API Gateway and Amazon EC2
- ✅ Amazon API Gateway and AWS Lambda

Explanation:-The Architect requires a solution that removes the need to manage instances. Therefore it must be a serverless service which rules out EC2. The two remaining options use AWS Lambda at the back-end for processing. Though CloudFront can trigger Lambda functions it is more suited to customizing content delivered from an origin. Therefore API Gateway with AWS Lambda is the most workable solution presented This solution will likely require other services such as S3 for content and a database service. Refer to the link below for an example scenario that use API Gateway and AWS Lambda with other services to create a serverless web application References: https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/

Q29)

A company is generating large datasets with millions of rows that must be summarized by column. Existing business intelligence tools will be used to build daily reports.

Which storage service meets the requirements?

- Amazon DynamoDB
- Amazon RDS
- Amazon ElastiCache
- ✅ Amazon RedShift

Explanation:-Amazon RedShift uses columnar storage and is used for analyzing data using business intelligence tools (SQL) Amazon RDS is more suited to OLTP workloads rather than analytics workloads Amazon ElastiCache is an in-memory caching service Amazon DynamoDB is a fully managed NoSQL database service, it is not a columnar database References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

Q30)

An application architect has requested some assistance with selecting a database for a new data warehouse requirement. The database must provide high performance and scalability. The data will be structured and persistent and the DB must support complex queries using SQL and BI tools.

Which AWS service will you recommend?

- ✅ RedShift

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 a SQL based data warehouse that is used for analytics applications. RedShift is 10x faster than a traditional SQL DB DynamoDB is a NoSQL database and so is not used for SQL ElastiCache is not a data warehouse, it is an in-memory database RDS is a relational database (SQL) but is used for transactional database implementations not data warehouses References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

- RDS
- DynamoDB
- ElastiCache

Q31) You are deploying an application on Amazon EC2 that must call AWS APIs. Which method of securely passing credentials to the application should you use?

- Store the API credentials on the instance using instance metadata
- Store API credentials as an object in Amazon S3
- Embed the API credentials into your application files
- ✅ Assign IAM roles to the EC2 instances

Explanation:-Always use IAM roles when you can It is an AWS best practice not to store API credentials within applications, on file systems or on instances (such as in metadata). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

Q32)

You work as a System Administrator at Digital Cloud Training and your manager has asked you to investigate an EC2 web

server hosting videos that is constantly running at over 80% CPU utilization.

Which of the approaches below would you recommend to fix the issue?

✅ Create a CloudFront distribution and configure the Amazon EC2 instance as the origin

Explanation:-Using the CloudFront content delivery network (CDN) would offload the processing from the EC2 instance as the videos would be cached and accessed without hitting the EC2 instance CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. CloudFront is a good choice for distribution of frequently accessed static content that benefits from edge delivery—like popular website images, videos, media files or software downloads. 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 Route53) – can also be external (non-AWS) Using CloudFront is preferable to using an Auto Scaling group to launch more instances as it is designed for caching content and would provide the best user experience Creating an ELB will not help unless there a more instances to distributed the load to References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

- Create an Elastic Load Balancer and register the EC2 instance to it
- Create a Launch Configuration from the instance using the CreateLaunchConfiguration action
- Create an Auto Scaling group from the instance using the CreateAutoScalingGroup action

---

Q33)

Your 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 S3. Each user will have a folder in a shared bucket under the folder structure: bucket/home/%username%.

What steps do you need to take to ensure that each user can access their own home folder and no one else's? (choose all that apply)

✅ Create an IAM group and attach the IAM policy

Explanation:-The AWS blog URL below explains how to construct an IAM policy for a similar scenario References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/ https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/

- Create an IAM policy that applies object-level S3 ACLs
- Create a bucket policy that applies access permissions based on username
- ✅ Create an IAM policy that applies folder-level permissions

Explanation:-The AWS blog URL below explains how to construct an IAM policy for a similar scenario References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/ https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/

Q34)

You are a Solutions Architect at Digital Cloud Training. You have just completed the implementation of a 2-tier web application for a client. The application uses EC2 instances, ELB and Auto Scaling across two subnets. After deployment you notice that only one subnet has EC2 instances running in it.

What might be the cause of this situation?

- The ELB is configured as an internal-only load balancer
- ✅ The Auto Scaling Group has not been configured with multiple subnets

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 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 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 If the AMI was missing from the launch configuration no instances would be running References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- Cross-zone load balancing is not enabled on the ELB
- The AMI is missing from the ASG's launch configuration

Q35)

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? (choose 2)

✅ Verify that the IAM instance profile has the necessary permissions

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 know 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. You apply IAM roles (instance profile) to EC2 instances, not groups This example is based on the EC2 launch type not the Fargate launch type. With Fargate the infrastructure is managed for you by AWS 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 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/ https://aws.amazon.com/premiumsupport/knowledge-center/ecs-agent-disconnected/

- Verify that the instances have the correct IAM group applied
- Verify that the container instances are using the Fargate launch type
- ✅ Verify that the container agent is running on the container instances

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 know 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. You apply IAM roles (instance profile) to EC2 instances, not groups This example is based on the EC2 launch type not the Fargate launch type. With Fargate the infrastructure is managed for you by AWS 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 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/ https://aws.amazon.com/premiumsupport/knowledge-center/ecs-agent-disconnected/

Q36)

A three-tier web application that you deployed in your VPC has been experiencing heavy load on the DB tier. The DB tier uses RDS MySQL in a multi-AZ configuration. Customers have been complaining about poor response times and you have been asked to find a solution. During troubleshooting you discover that the DB tier is experiencing high read contention during peak hours of the day.

What are two possible options you could use to offload some of the read traffic from the DB to resolve the performance issues? (choose 2)

✅ Deploy ElastiCache in each AZ

Explanation:-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 Moving from a relational DB to a NoSQL DB (DynamoDB) is unlikely to be a viable solution 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://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

⚪ Use an ELB to distribute load between RDS instances

⚪ Migrate to DynamoDB

✅ Add RDS read replicas in each AZ

Explanation:-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 Moving from a relational DB to a NoSQL DB (DynamoDB) is unlikely to be a viable solution 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://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

Q37)

A company runs several web applications on AWS that experience a large amount of traffic. An Architect is considering adding a caching service to one of the most popular web applications.

What are two advantages of using ElastiCache? (choose 2)

✅ Can be used for storing session state data

Explanation:-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 Elasticache can also be used for storing session state You cannot enable multi-region HA with ElastiCache ElastiCache is a caching service, not a network service so it is not responsible for providing low-latency network connectivity Amazon SQS is used for decoupling application components References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/

⚪ Decoupling application components

✅ Caching query results for improved performance

Explanation:-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 Elasticache can also be used for storing session state You cannot enable multi-region HA with ElastiCache ElastiCache is a caching service, not a network service so it is not responsible for providing low-latency network connectivity Amazon SQS is used for decoupling application components References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/

⚪ Multi-region HA

Q38)

The development team in your company have created a Python application running on ECS containers with the Fargate launch type. You have created an ALB 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. You would like to securely authenticate the users on the front-end before they access the authenticated portions of the application.

How can this be done on the ALB?

⚪ This cannot be done on an ALB; you'll need to authenticate users on the back-end with AWS Single Sign-On (SSO) integration

⚪ This cannot be done on an ALB; you'll need to use another layer in front of the ALB

⚪ The only option is to use SAML with Amazon Cognito on the ALB

✅ 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

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 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://aws.amazon.com/blogs/aws/built-in-authentication-in-alb/

Q39) You are concerned that you may be getting close to some of the default service limits for several AWS services. What AWS tool can be used to display current usage and limits?

⚪ AWS Dashboard

✅ AWS Trusted Advisor

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 AWS CloudWatch is used for performance monitoring not displaying usage limits 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 There is no service known as "AWS Dashboard" References: https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html

- AWS Systems Manager
- AWS CloudWatch

Q40)

A company is deploying new services on EC2 and needs to determine which instance types to use with what type of attached storage.

Which of the statements about Instance store-backed and EBS-backed instances is true?

- Instance-store backed instances can be stopped and restarted
- Instance-store backed instances can only be terminated
- ✅ EBS-backed instances can be stopped and restarted

Explanation:-EBS-backed means the root volume is an EBS volume and storage is persistent whereas instance store-backed means the root volume is an instance store volume and storage is not persistent On an EBS-backed instance, the default action is for the root EBS volume to be deleted upon termination EBS backed instances can be stopped. You will not lose the data on this instance if it is stopped (persistent) EBS volumes can be detached and reattached to other EC2 instances EBS volume root devices are launched from AMI's that are backed by EBS snapshots Instance store volumes are sometimes called Ephemeral storage (non-persistent) Instance store volumes cannot be stopped. If the underlying host fails the data will be lost Instance store volume root devices are created from AMI templates stored on S3 Instance store volumes cannot be detached/reattached When rebooting the instances for both types data will not be lost By default both root volumes will be deleted on termination unless you configured otherwise References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

- EBS-backed instances cannot be restarted

Q41) You are trying to clean up your 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?

- You must retain all snapshots as the process is incremental and therefore data is required from each snapshot
- The oldest snapshot, as this references data in all other snapshots
- Two snapshots, the oldest and most recent snapshots
- ✅ Only the most recent snapshot. Snapshots are incremental, but the deletion process will ensure that no data is lost

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 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-snapshot.html

---

Q42)

You are running an application on EC2 instances in a private subnet of your VPC. You would like to connect the application to Amazon API Gateway. For security reasons, you need to ensure that no traffic traverses the Internet and need to ensure all traffic uses private IP addresses only.

How can you achieve this?

- Add the API gateway to the subnet the EC2 instances are located in
- Create a public VIF on a Direct Connect connection
- Create a NAT gateway
- ✅ Create a private API using an interface VPC endpoint

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 You do not need to implement Direct Connect and create a public VIF. This would not ensure that traffic avoids the Internet You cannot add API Gateway to the subnet the EC2 instances are in, it is a public service with a public endpoint NAT Gateways are used to provide Internet access for EC2 instances in public subnets so are of no use in this solution References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q43)

You need to create a file system that can be concurrently accessed by multiple EC2 instances within an AZ. 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 you need to ensure it is encrypted at rest and in transit.

Which storage solution would you implement for the EC2 instances?

- Use the Elastic Block Store (EBS) and mount the file system at the block level
- ✅ Use the Elastic File System (EFS) and mount the file system using NFS v4.1

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 EBS is a block-level storage system not a file-level storage system. You cannot connect to a single EBS volume concurrently from multiple EC2 instances 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 You cannot use an ELB to distribute data between EBS volumes References: https://digitalcloud.training/certification-training/aws-solutions-architect-

associate/storage/amazon-efs/

- Add EBS volumes to each EC2 instance and configure data replication
- Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

---

Q44)

The development team in your organization would like to start leveraging AWS services. They have asked you what AWS service can be used to quickly deploy and manage applications in the AWS Cloud? The developers would like the ability to simply upload applications and have AWS handle the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

What AWS service would you recommend?

- EC2
- OpsWorks
- Auto Scaling
- ✅ Elastic Beanstalk

Explanation:-Whenever you hear about developers uploading code/applications think Elastic Beanstalk.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 supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker web applications If you use EC2 you must manage the deployment yourself, AWS will not handle the deployment, capacity provisioning etc. Auto Scaling does not assist with deployment of applications OpsWorks provides a managed Chef or Puppet infrastructure. You can define how to deploy and configure infrastructure but it does not give you the ability to upload application code and have the service deploy the application for you References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/

Q45) 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? (choose 2)

- System Events which are also known as instance level operations
- ✅ Data Events which are also known as data plane operations

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 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudtrail/ https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-management-and-data-events-with-cloudtrail.html

- Platform Events which are also known as hardware level operations
- ✅ Management Events which are also known as control plane operations

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 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudtrail/ https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-management-and-data-events-with-cloudtrail.html

---

Q46)

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?

- Continuous replication
- ✅ Synchronous replication

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) Asynchronous replication is used by RDS for Read Replicas Scheduled and continuous replication are not replication types that are supported by RDS References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- Asynchronous replication
- Scheduled replication

Q47)

You have an existing Auto Scaling Group running with 8 EC2 instances. You have decided to attach an ELB to the ASG by connecting a Target Group. The ELB is in the same region and already has 10 EC2 instances running in the Target Group.

When attempting to attach the ELB the request immediately fails, what is the MOST likely cause?

- You cannot attach running EC2 instances to an ASG
- ASGs cannot be edited once defined, you would need to recreate it
- One or more of the instances are unhealthy
- ✅ Adding the 10 EC2 instances to the ASG would exceed the maximum capacity configured

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 Auto Scaling Groups can be edited once created (however launch configurations cannot be edited) You can attach running EC2 instances to an ASG 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 References: https://digitalcloud.training/certification-training/aws-

solutions-architect-associate/compute/aws-auto-scaling/ https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html

---

Q48)

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? (choose 2)

- VPC endpoint
- ✓ CloudFront distribution

Explanation:-Alias records are used to map resource record sets in your hosted zone to Amazon Elastic Load Balancing load balancers, Amazon CloudFront distributions, AWS Elastic Beanstalk environments, or Amazon S3 buckets that are configured as websites 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) You cannot use an Alias to point at an ElastiCache cluster or VPC endpoint References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/ https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

- On-premise web server
- ✓ Elastic BeanStalk environment

Explanation:-Alias records are used to map resource record sets in your hosted zone to Amazon Elastic Load Balancing load balancers, Amazon CloudFront distributions, AWS Elastic Beanstalk environments, or Amazon S3 buckets that are configured as websites 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) You cannot use an Alias to point at an ElastiCache cluster or VPC endpoint References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/ https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

---

Q49)

Your organization has a data lake on S3 and you need 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? (choose 2)

- AWS Glue for the ad hoc SQL querying
- ✓ RedShift Spectrum for the complex queries

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 AWS Lambda is a serverless technology for running functions, it is not the best solution for running analytics queries AWS Glue is an ETL service 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/

- ✓ Amazon Athena for the ad hoc SQL querying

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 AWS Lambda is a serverless technology for running functions, it is not the best solution for running analytics queries AWS Glue is an ETL service 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/

- AWS Lambda for the complex queries

Q50)

You are a Solutions Architect at Digital Cloud Training and have been assigned the task of moving some sensitive documents into the AWS cloud. You need to ensure that the security of the documents is maintained.

Which AWS features can help ensure that the sensitive documents are secured on the AWS cloud? (choose 2)

- ✓ EBS encryption with Customer Managed Keys

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. 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 IAM access policies are not used for controlling encryption 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 S3 cross-region replication can be used for fault tolerance but does not apply any additional security to the data References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- S3 cross region replication
- EBS snapshots
- ✓ S3 Server-Side Encryption

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. 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 IAM access policies are not used for controlling encryption 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 S3 cross-region replication can be used for fault tolerance but does not apply any additional security to the data References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/
