Answer Sheet

Q1) You are creating a CloudFormation template that will provision a new EC2 instance and new EBS volume. What do you need to specify to associate the block store with the instance?

- The EC2 logical ID
- Both the EC2 physical ID and the EBS physical ID
- The EC2 physical ID
- ✅ Both the EC2 logical ID and the EBS logical ID

Explanation:-Logical IDs are used to reference resources within the template Physical IDs identify resources outside of AWS CloudFormation templates, but only after the resources have been created References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/

Q2)

A health club is developing a mobile fitness app that allows customers to upload statistics and view their progress. Amazon Cognito is being used for authentication, authorization and user management and users will 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?

- Key Pairs
- SAML Identity Providers
- User Pools
- ✅ Identity Pools

Explanation:-With an identity pool, users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB 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) SAML Identity Providers are supported IDPs for identity pools but cannot be used for gaining temporary credentials for AWS services Key pairs are used in Amazon EC2 for access to instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

Q3) You are discussing EC2 with a colleague and need to describe the differences between EBS-backed instances and Instance store-backed instances. Which of the statements below would be valid descriptions? (choose 2)

- ✅ On an EBS-backed instance, the default action is for the root EBS volume to be deleted upon termination

Explanation:-On an EBS-backed instance, the default action is for the root EBS volume to be deleted upon termination EBS volumes can be detached and reattached to other EC2 instances Instance store volumes cannot be detached and reattached to other EC2 instances When rebooting the instances for both types data will not be lost By default, root volumes for both types will be deleted on termination unless you configured otherwise References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

- Instance store volumes can be detached and reattached to other EC2 instances
- By default, root volumes for both types will be retained on termination unless you configured otherwise
- ✅ EBS volumes can be detached and reattached to other EC2 instances

Explanation:-On an EBS-backed instance, the default action is for the root EBS volume to be deleted upon termination EBS volumes can be detached and reattached to other EC2 instances Instance store volumes cannot be detached and reattached to other EC2 instances When rebooting the instances for both types data will not be lost By default, root volumes for both types will be deleted on termination unless you configured otherwise References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

Q4)

An Auto Scaling group is configured with the default termination policy. The group spans multiple Availability Zones and each AZ has the same number of instances running.

A scale in event needs to take place, what is the first step in evaluating which instances to terminate?

- Select the newest instance in the group
- Select instances that are closest to the next billing hour
- ✅ Select instances that use the oldest launch configuration

Explanation:-Using the default termination policy, when there are even number of instances in multiple AZs, Auto Scaling will first select the instances with the oldest launch configuration, and if multiple instances share the oldest launch configuration, AS then selects the instances that are closest to the next billing hour References: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

- Select instances randomly

Q5) A new application you are deploying uses Docker containers. You are creating a design for an ECS cluster to host the application. Which statements about ECS clusters are correct? (choose 2)

- Each container instance may be part of multiple clusters at a time
- ✅ Clusters can contain tasks using the Fargate and EC2 launch type

Explanation:-ECS Clusters are a logical grouping of container instances the you can place tasks on Clusters can contain tasks using BOTH the Fargate and EC2 launch type Each container instance may only be part of one cluster at a time Clusters are region specific For clusters with the EC2 launch type clusters can contain different container instance types References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

- ✅ ECS Clusters are a logical grouping of container instances that you can place tasks on

Explanation:-ECS Clusters are a logical grouping of container instances the you can place tasks on Clusters can contain tasks using BOTH the Fargate and EC2 launch type Each container instance may only be part of one cluster at a time Clusters are region specific For clusters with the EC2 launch type clusters can contain different container instance types References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

- Clusters are AZ specific

Q6)

An Auto Scaling Group in which you have four EC2 instances running is becoming heavily loaded. The instances are using the m4.large instance type and the CPUs are hitting 80%. Due to licensing constraints you don't want to add additional instances to the ASG so you are planning to upgrade to the m4.xlarge instance type instead. You need to make the change immediately but don't want to terminate the existing instances.

How can you perform the change without causing the ASG to launch new instances? (choose 2)

- ✅ On the ASG suspend the Auto Scaling process until you have completed the change

Explanation:-When you resize an instance, you must select an instance type that is compatible with the configuration of the instance. You must stop your Amazon EBS–backed instance before you can change its instance type You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. 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 You do not need to create a new launch configuration and you cannot edit an existing launch configuration You cannot change an instance type without first stopping the instance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html

- Create a new launch configuration with the new instance type specified
- Change the instance type and then restart the instance
- ✅ Stop each instance and change its instance type. Start the instance again

Explanation:-When you resize an instance, you must select an instance type that is compatible with the configuration of the instance. You must stop your Amazon EBS–backed instance before you can change its instance type You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. 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 You do not need to create a new launch configuration and you cannot edit an existing launch configuration You cannot change an instance type without first stopping the instance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html

---

Q7) 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?

- Amazon SQS
- ✅ Amazon SWF

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 Amazon Security Token Service (STS) is used for requesting temporary credentials Amazon Simple Queue Service (SQS) is a message queue used for decoupling application components 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://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-swf/

- Amazon SNS
- Amazon STS

Q8)

You are building a new Elastic Container Service (ECS) cluster. The ECS instances are running the EC2 launch type and you would like to enable load balancing to distributed connections to the tasks running on the cluster. You would like the mapping of ports to be performed dynamically and will need to route to different groups of servers based on the path in the requested URL.

Which AWS service would you choose to fulfil these requirements?

- Network Load Balancer
- ECS Services
- ✅ Application Load Balancer

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 – the CLB and NLB do not offer this An ALB can also route requests based on the content of the request in the host field: host-based or path-based References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://aws.amazon.com/premiumsupport/knowledge-center/dynamic-port-mapping-ecs/ https://docs.aws.amazon.com/elasticloadbalancing/latest/application/tutorial-load-balancer-routing.html

- Classic Load Balancer

Q9) In your AWS VPC, you need to add a new subnet that will allow you to host a total of 20 EC2 instances.Which of the following IPv4 CIDR blocks can you use for this scenario?

- 172.0.0.0/28
- 172.0.0.0/30
- 172.0.0.0/29
- ✅ 172.0.0.0/27

Explanation:-When you create a VPC, you must specify an IPv4 CIDR block for the VPC The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses) The CIDR block must not overlap with any existing CIDR block that's associated with the VPC A /27 subnet mask provides 32 addresses The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance The following list shows total addresses for different subnet masks: /32 = 1 ; /31 = 2 ; /30 = 4 ; /29 = 8 ; /28 = 16 ; /27 = 32 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q10)

You created a second ENI (eth1) interface when launching an EC2 instance. You would like to terminate the instance and have

not made any changes.

What will happen to the attached ENIs?

- Both eth0 and eth1 will persist
- eth1 will be terminated, but eth0 will persist
- ✅ eth1 will persist but eth0 will be terminated

Explanation:-By default Eth0 is the only Elastic Network Interface (ENI) created with an EC2 instance when launched. You can add additional interfaces to EC2 instances (number dependent on instances family/type). Default interfaces are terminated with instance termination. Manually added interfaces are not terminated by default References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

- Both eth0 and eth1 will be terminated with the instance

Q11) You are designing solutions that will utilize CloudFormation templates and your manager has asked how much extra will it cost to use CloudFormation to deploy resources?

- ✅ There is no additional charge for AWS CloudFormation, you only pay for the AWS resources that are created

Explanation:-There is no additional charge for AWS CloudFormation. You pay for AWS resources (such as Amazon EC2 instances, Elastic Load Balancing load balancers, etc.) created using AWS CloudFormation in the same manner as if you created them manually. You only pay for what you use, as you use it; there are no minimum fees and no required upfront commitments There is no flat fee, per hour usage costs or charges applicable to templates References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/

- The cost is based on the size of the template
- CloudFormation is charged per hour of usage
- Amazon charge a flat fee for each time you use CloudFormation

---

Q12) You would like to store a backup of an Amazon EBS volume on Amazon S3. What is the easiest way of achieving this?

- ✅ Create a snapshot of the volume

Explanation:-Snapshots capture a point-

- Write a custom script to automatically copy your data to an S3 bucket
- Use SWF to automatically create a backup of your EBS volumes and then upload them to an S3 bucket
- You don't need to do anything, EBS volumes are automatically backed up by default

---

Q13)

You are a Solutions Architect for a systems integrator. Your client is growing their presence in the AWS cloud and has applications and services running in a VPC across multiple availability zones within a region. The client has a requirement to build an operational dashboard within their on-premise data center within the next few months. The dashboard will show near real time statistics and therefore must be connected over a low latency, high performance network.

What would be the best solution for this requirement?

- You cannot connect to multiple AZs from a single location
- Use redundant VPN connections to two VGW routers in the region, this should give you access to the infrastructure in all AZs
- Order multiple AWS Direct Connect connections that will be connected to multiple AZs
- ✅ Order a single AWS Direct Connect connection to connect to the client's VPC. This will provide access to all AZs within the region

Explanation:-With AWS Direct Connect you can provision a low latency, high performance private connection between the client's data center and AWS. Direct Connect connections connect you to a region and all AZs within that region. In this case the client has a single VPC so we know their resources are container within a single region and therefore a single Direct Connect connection satisfies the requirements. As Direct Connect connections allow you to connect to all AZs within a region you do not need to order multiple connections (but you might want to for redundancy) VPN connections use the public Internet and are therefore not good when you need a low latency, high performance and consistent network experience References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/

Q14) Your client is looking for a way to use standard templates for describing and provisioning their infrastructure resources on AWS. Which AWS service can be used in this scenario?

- Auto Scaling
- Simple Workflow Service (SWF)
- Elastic Beanstalk
- ✅ CloudFormation

Explanation:-AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion. AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment AWS Auto Scaling is used for providing elasticity to EC2 instances by launching or terminating instances based on load Elastic Beanstalk is a PaaS service for running managed web applications. It is not used for infrastructure deployment Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components, it does not use templates for deploying infrastructure References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/

Q15)

An application that you will be deploying in your VPC requires 14 EC2 instances that must be placed on distinct underlying hardware to reduce the impact of the failure of a hardware node. The instances will use varying instance types.

What configuration will cater to these requirements taking cost-effectiveness into account?

- ✅ Use a Spread Placement Group across two AZs

Explanation:-A spread placement group is a group of instances that are each placed on distinct underlying hardware. Spread placement groups are

recommended for applications that have a small number of critical instances that should be kept separate from each other. Launching instances in a spread placement group reduces the risk of simultaneous failures that might occur when instances share the same underlying hardware A cluster placement group is a logical grouping of instances within a single Availability Zone. Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both, and if the majority of the network traffic is between the instances in the group Using a single instance on each dedicated host would be extremely expensive References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

- Use dedicated hosts and deploy each instance on a dedicated host
- You cannot control which nodes your instances are placed on
- Use a Cluster Placement Group within a single AZ

Q16)

A new mobile application that your company is deploying will be hosted on AWS. The users of the application will use mobile devices to upload small amounts of data on a frequent basis. It is expected that the number of users connecting each day could be over 1 million. The data that is uploaded must be stored in a durable and persistent data store.

The data store must also be highly available and easily scalable.

Which AWS services would you use?

- ✅ DynamoDB

Explanation:-Amazon DynamoDB is a fully managed NoSQL database service that provides a durable and persistent data store. You can scale DynamoDB using push button scaling which means that you can scale the DB at any time without incurring downtime. Amazon DynamoDB stores three geographically distributed replicas of each table to enable high availability and data durability RedShift is a data warehousing solution that is used for analytics on data, it is not used for transactional databases RDS is not highly available unless you use multi-AZ, which is not specified in the answer. It is also harder to scale RDS as you must change the instance size and incur downtime Kinesis is used for collecting, processing and analyzing streaming data. It is not used as a data store References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

- RDS
- Kinesis
- RedShift

Q17)

A Solutions Architect is responsible for a web application that runs on EC2 instances that sit behind an Application Load Balancer (ALB). Auto Scaling is used to launch instances across 3 Availability Zones. The web application serves large image files and these are stored on an Amazon EFS file system. Users have experienced delays in retrieving the files and the Architect has been asked to improve the user experience.

What should the Architect do to improve user experience?

- Reduce the file size of the images
- ✅ Cache static content using CloudFront

Explanation:-CloudFront is ideal for caching static content such as the files in this scenario and would increase performance Moving the files to EBS would not make accessing the files easier or improve performance Reducing the file size of the images may result in better retrieval times, however CloudFront would still be the preferable option Using Spot EC2 instances may reduce EC2 costs but it won't improve user experience References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

- Move the digital assets to EBS
- Use Spot instances

Q18)

A Solutions Architect needs to transform data that is being uploaded into S3. The uploads happen sporadically and the transformation should be triggered by an event. The transformed data should then be loaded into a target data store.

What services would be used to deliver this solution in the MOST cost-effective manner? (choose 2)

- Configure CloudFormation to provision a Kinesis data stream to transform the data and load it into S3
- ✅ Use AWS Glue to extract, transform and load the data into the target data store

Explanation:-S3 event notifications triggering a Lambda function is completely serverless and cost-effective AWS Glue can trigger ETL jobs that will transform that data and load it into a data store such as S3 Kinesis Data Streams is used for processing data, rather than extracting and transforming it. The Kinesis consumers are EC2 instances which are not as cost-effective as serverless solutions AWS Data Pipeline can be used to automate the movement and transformation of data, it relies on other services to actually transform the data References: https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html https://aws.amazon.com/glue/

- Configure a CloudWatch alarm to send a notification to CloudFormation when data is uploaded
- ✅ Configure S3 event notifications to trigger a Lambda function when data is uploaded and use the Lambda function to trigger the ETL job

Explanation:-S3 event notifications triggering a Lambda function is completely serverless and cost-effective AWS Glue can trigger ETL jobs that will transform that data and load it into a data store such as S3 Kinesis Data Streams is used for processing data, rather than extracting and transforming it. The Kinesis consumers are EC2 instances which are not as cost-effective as serverless solutions AWS Data Pipeline can be used to automate the movement and transformation of data, it relies on other services to actually transform the data References: https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html https://aws.amazon.com/glue/

Q19)

A Solutions Architect is developing an encryption solution. The solution requires that data keys are encrypted using envelope protection before they are written to disk.

Which solution option can assist with this requirement?

- AWS Certificate Manager
- ✅ AWS KMS API

Explanation:-The AWS KMS API can be used for encrypting data keys (envelope encryption) AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users) IAM access keys are used for signing programmatic requests you make to AWS References: https://docs.aws.amazon.com/kms/latest/APIReference/Welcome.html

- API Gateway with STS
- IAM Access Key

Q20)

A Solutions Architect has been asked to suggest a solution for analyzing data in S3 using standard SQL queries. The solution should use a serverless technology.

Which AWS service can the Architect use?

- Amazon RedShift
- ✅ Amazon Athena

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 RedShift is used for analytics but cannot analyze data in S3 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. It is not used for analyzing data in S3 AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals References: https://aws.amazon.com/athena/

- AWS Glue
- AWS Data Pipeline

Q21)

An application you manage stores encrypted data in S3 buckets. You need to be able to query the encrypted data using SQL queries and write the encrypted results back the S3 bucket. As the data is sensitive you need to implement fine-grained control over access to the S3 bucket.

What combination of services represent the BEST options support these requirements? (choose 2)

- Use bucket ACLs to restrict access to the bucket
- ✅ Use IAM policies to restrict access to the bucket

Explanation:-Athena also 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 With IAM policies, you can grant IAM users fine-grained control to your S3 buckets, and is preferable to using bucket ACLs AWS Glue is an ETL service and is not used for querying and analyzing data in S3 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/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

- ✅ Use Athena for querying the data and writing the results back to the bucket

Explanation:-Athena also 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 With IAM policies, you can grant IAM users fine-grained control to your S3 buckets, and is preferable to using bucket ACLs AWS Glue is an ETL service and is not used for querying and analyzing data in S3 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/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

- Use AWS Glue to extract the data, analyze it, and load it back to the S3 bucket

---

Q22)

An application tier of a multi-tier web application currently hosts two web services on the same set of instances. The web services each listen for traffic on different ports.

Which AWS service should a Solutions Architect use to route traffic to the service based on the incoming request path?

- Classic Load Balancer (CLB)
- Amazon Route 53
- ✅ Application Load Balancer (ALB)

Explanation:-An Application Load Balancer is a type of Elastic Load Balancer that can use layer 7 (HTTP/HTTPS) protocol data to make forwarding decisions. An ALB supports both path-based (e.g. /images or /orders) and host-based routing (e.g. example.com) In this scenario a single EC2 instance is listening for traffic for each application on a different port. You can use a target group that listens on a single port (HTTP or HTTPS) and then uses listener rules to selectively route to a different port on the EC2 instance based on the information in the URL path. So you might have example.com/images going to one back-end port and example.com/orders going to a different back0end port You cannot use host-based or path-based routing with a CLB Amazon CloudFront caches content, it does not direct traffic to different ports on EC2 instances Amazon Route 53 is a DNS service. It can be used to load balance however it does not have the ability to route based on information in the incoming request path References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- Amazon CloudFront

Q23)

An application runs on two EC2 instances in private subnets split between two AZs. The application needs to connect to a CRM SaaS application running on the Internet. The vendor of the SaaS application restricts authentication to a whitelist of source IP addresses and only 2 IP addresses can be configured per customer.

What is the most appropriate and cost-effective solution to enable authentication to the SaaS application?

- Configure redundant Internet Gateways and update the routing tables for each subnet
- Use multiple Internet-facing Application Load Balancers with Elastic IP addresses

✅ Configure a NAT Gateway for each AZ with an Elastic IP address

Explanation:-In this scenario you need to connect the EC2 instances to the SaaS application with a source address of one of two whitelisted public IP addresses to ensure authentication works. A NAT Gateway is created in a specific AZ and can have a single Elastic IP address associated with it. NAT Gateways are deployed in public subnets and the route tables of the private subnets where the EC2 instances reside are configured to forward Internet-bound traffic to the NAT Gateway. You do pay for using a NAT Gateway based on hourly usage and data processing, however this is still a cost-effective solution A Network Load Balancer can be configured with a single static IP address (the other types of ELB cannot) for each AZ. However, using a NLB is not an appropriate solution as the connections are being made outbound from the EC2 instances to the SaaS app and ELBs are used for distributing inbound connection requests to EC2 instances (only return traffic goes back through the ELB) An ALB does not support static IP addresses and is not suitable for a proxy function AWS Route 53 is a DNS service and is not used as an outbound proxy server so is not suitable for this scenario References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

⚪ Use a Network Load Balancer and configure a static IP for each AZ

Q24)

The website for a new application received around 50,000 requests each second and the company wants to use multiple applications to analyze the navigation patterns of the users on their website so they can personalize the user experience.

What can a Solutions Architect use to collect page clicks for the website and process them sequentially for each user?

⚪ Amazon SQS FIFO queue

✅ Amazon Kinesis Streams

Explanation:-This is a good use case for Amazon Kinesis streams as it is able to scale to the required load, allow multiple applications to access the records and process them sequentially Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications Amazon Kinesis streams allows up to 1 MiB of data per second or 1,000 records per second for writes per shard. There is no limit on the number of shards so you can easily scale Kinesis Streams to accept 50,000 per second 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 Standard SQS queues do not ensure that messages are processed sequentially and FIFO SQS queues do not scale to the required number of transactions a second CloudTrail is used for auditing an is not useful here. References: https://docs.aws.amazon.com/streams/latest/dev/service-sizes-and-limits.html https://aws.amazon.com/kinesis/data-streams/faqs/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

⚪ Amazon SQS standard queue

⚪ AWS CloudTrail trail

Q25)

An AWS user has created a Provisioned IOPS EBS volume which is attached to an EBS optimized instance and configured 1000 IOPS.

Based on the EC2 SLA, what is the average IOPS the user will achieve for most of the year?

⚪ 1000

⚪ 950

⚪ 990

✅ 900

Explanation:-Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year. Therefore you should expect to get 900 IOPS most of the year. References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

---

Q26) Which of the following approaches provides the lowest cost for Amazon elastic block store snapshots while giving you the ability to fully restore data?

✅ Maintain a single snapshot; the latest snapshot is both incremental and complete

Explanation:-You can backup data on an EBS volume by periodically taking snapshots of the volume. The scenario is that you need to reduce storage costs by maintaining as few EBS snapshots as possible whilst ensuring you can restore all data when required. If you take periodic snapshots of a volume, the snapshots are incremental which means 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 such that you need to retain only the most recent snapshot in order to restore the volume You cannot just keep the original snapshot as it will not be incremental and complete You do not need to keep the original and latest snapshot as the latest snapshot is all that is needed There is no need to archive the original snapshot to Amazon Glacier. EBS copies your data across multiple servers in an AZ for durability References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

⚪ Maintain the original snapshot; subsequent snapshots will overwrite one another

⚪ Maintain two snapshots: the original snapshot and the latest incremental snapshot

⚪ Maintain the most current snapshot; archive the original to Amazon Glacier

---

Q27)

You are a Solutions Architect at Digital Cloud Training. One of your clients is expanding their operations into multiple AWS regions around the world. The client has requested some advice on how to leverage their existing AWS Identity and Access Management (IAM) configuration in other AWS regions.

What advice would you give to your client?

⚪ The client will need to create a VPC peering configuration with each remote AWS region and then allow IAM access across regions

⚪ The client can use Amazon Cognito to create a single sign-on configuration across multiple AWS regions

✅ IAM is a global service and the client can use users, groups, roles, and policies in any AWS region

Explanation:-IAM is universal (global) and does not apply to regions so you will use the same IAM configuration no matter if you use one of all regions VPC peering is not required Amazon Cognito is used for authentication with web and mobile apps, it is not required to make IAM work across

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

- IAM is a regional service and the client will need to copy the configuration items required across to other AWS regions

---

Q28)

You have deployed a highly available web application across two AZs. The application uses an Auto Scaling Group (ASG) and an Application Load Balancer (ALB) to distribute connections between the EC2 instances that make up the web front-end. The load has increased and the ASG has launched new instances in both AZs, however you noticed that the ALB is only distributing traffic to the EC2 instances in one AZ.

From the options below, what is the most likely cause of the issue?

- The ASG has not registered the new instances with the ALB
- The EC2 instances in one AZ are not passing their health checks
- Cross-zone load balancing is not enabled on the ALB
- ✅ The ALB does not have a public subnet defined in both AZs

Explanation:-Cross-zone load balancing is enabled on the ALB by default. Also, if it was disabled the ALB would send traffic equally to each AZ configured regardless of the number of hosts in each AZ so some traffic would still get through Internet facing 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 The ASG would automatically register new instances with the ALB EC2 instance health checks are unlikely to be the issue here as the instances in both AZs are all being launched from the same ASG so should be identically configured Please refer to the AWS article linked below for detailed information on the configuration described in this scenario References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

Q29)

One of your clients has asked you for some advice on an issue they are facing regarding storage. The client uses an on-premise block based storage array which is getting close to capacity. The client would like to maintain a configuration where reads/writes to a subset of frequently accessed data are performed on-premise whilst also alleviating the local capacity issues by migrating data into the AWS cloud.

What would you suggest as the BEST solution to the client's current problems?

- Archive data that is not accessed regularly straight into Glacier
- Use S3 copy command to copy data into the AWS cloud
- ✅ Implement a Storage Gateway Volume Gateway in cached mode

Explanation:-Backing up the data and then deleting it is not the best solution when much of the data is accessed regularly A Storage Gateway Volume Gateway in cached mode will store the entire dataset on S3 and a cache of the most frequently accessed data is cached on-site The S3 copy command doesn't help here as the data is not in S3 You cannot archive straight into Glacier, you must store data on S3 first. Also, archiving is not the best solution to this problem References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/

- Implement a Storage Gateway Virtual Tape Library, backup the data and then delete the data from the array

---

Q30)

You are a Solutions Architect at Digital Cloud Training. Your client's company is growing and now has over 10,000 users. The client would like to start deploying services into the AWS Cloud including AWS Workspaces. The client expects there to be a large take-up of AWS services across their user base and would like to use their existing Microsoft Active Directory identity source for authentication. The client does not want to replicate account credentials into the AWS cloud.You have been tasked with designing the identity, authorization and access solution for the customer.

Which AWS services will you include in your design? (choose 2)

- Use a Large AWS Simple AD
- ✅ Use the Enterprise Edition of AWS Directory Service for Microsoft Active Directory

Explanation:-The customer wants to leverage their existing directory but not replicate account credentials into the cloud. Therefore they can use the Active Directory Service for Microsoft Active Directory and create a trust relationship with their existing AD domain. This will allow them to authenticate using local user accounts in their existing directory without creating an AD Domain Controller in the cloud (which would entail replicating account credentials) Active Directory Service for Microsoft Active Directory is the best choice if you have more than 5000 users and/or need a trust relationship set up AWS Simple AD does not support trust relationships with other domains and therefore cannot be used in this situation AD Connector would be a good solution for this scenario, however it does not support the number of users in the organization (up to 5000 users only) Amazon Cognito is used for mobile and web app authentication References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

- Use an AWS Cognito user pool
- ✅ Setup trust relationships to extend authentication from the on-premises Microsoft Active Directory into the AWS cloud

Explanation:-The customer wants to leverage their existing directory but not replicate account credentials into the cloud. Therefore they can use the Active Directory Service for Microsoft Active Directory and create a trust relationship with their existing AD domain. This will allow them to authenticate using local user accounts in their existing directory without creating an AD Domain Controller in the cloud (which would entail replicating account credentials) Active Directory Service for Microsoft Active Directory is the best choice if you have more than 5000 users and/or need a trust relationship set up AWS Simple AD does not support trust relationships with other domains and therefore cannot be used in this situation AD Connector would be a good solution for this scenario, however it does not support the number of users in the organization (up to 5000 users only) Amazon Cognito is used for mobile and web app authentication References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

Q31)

An EC2 instance that you manage has an IAM role attached to it that provides it with access to Amazon S3 for saving log data to a bucket. A change in the application architecture means that you now need to provide the additional ability for the application to securely make API requests to Amazon API Gateway.

Which two methods could you use to resolve this challenge? (choose 2)

✅ Create a new IAM role with multiple IAM policies attached that grants access to Amazon S3 and Amazon API Gateway, and replace the existing IAM role that is attached to the EC2 instance

Explanation:-There are two possible solutions here. In one you create a new IAM role with multiple policies, in the other you add a new policy to the existing IAM role. Contrary to one of the incorrect answers, you can modify IAM roles after an instance has been launched - this was changed quite some time ago now. However, you cannot add multiple IAM roles to a single EC2 instance. If you need to attach multiple policies you must attach them to a single IAM role. There is no such thing as delegating access using the API Gateway management console References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

⚪ Delegate access to the EC2 instance from the API Gateway management console

⚪ Create an IAM role with a policy granting permissions to Amazon API Gateway and add it to the EC2 instance as an additional IAM role

✅ Add an IAM policy to the existing IAM role that the EC2 instance is using granting permissions to access Amazon API Gateway

Explanation:-There are two possible solutions here. In one you create a new IAM role with multiple policies, in the other you add a new policy to the existing IAM role. Contrary to one of the incorrect answers, you can modify IAM roles after an instance has been launched - this was changed quite some time ago now. However, you cannot add multiple IAM roles to a single EC2 instance. If you need to attach multiple policies you must attach them to a single IAM role. There is no such thing as delegating access using the API Gateway management console References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

Q32)

As a Solutions Architect for Digital Cloud Training you are designing an online shopping application for a new client. The application will be composed of distributed, decoupled components to ensure that the failure of a single component does not affect the availability of the application.You will be using SQS as the message queueing service and the client has stipulated that the messages related to customer orders must be processed in the order that they were submitted in the online application. The client expects that the peak rate of transactions will not exceed 140 transactions a second.

What will you explain to the client?

⚪ This is fine, standard SQS queues can guarantee the order of the messages

⚪ The only way this can be achieved is by configuring the applications to process messages from the queue in the right order based on timestamps

✅ This can be achieved by using a FIFO queue which will guarantee the order of messages

Explanation:-Queues can be either standard or first-in-first-out (FIFO) Standard queues provide a loose-FIFO capability that attempts to preserve the order of messages and provide at-least-once delivery, which means that each message is delivered at least once. Therefore you could not use a standard queue for this solution as it would not be guaranteed that the order of the messages would be maintained FIFO (first-in-first-out) queues preserve the exact order in which messages are sent and received.. If you use a FIFO queue, you don't have to place sequencing information in your message and they provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it. A FIFO queue would fit the solution requirements for this question Configuring the application to process messages from the queue based on timestamps is more complex and not necessary when you can implement FIFO queues References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/

⚪ This is not possible with SQS as you cannot control the order in the queue

---

Q33)

A Solutions Architect is designing a shared service for hosting containers from several customers on Amazon ECS. These containers will use several AWS services. A container from one customer must not be able to access data from another customer.

Which solution should the Architect use to meet the requirements?

✅ IAM roles for tasks

Explanation:-IAM roles for ECS tasks enabled you to secure your infrastructure by assigning an IAM role directly to the ECS task rather than to the EC2 container instance. This means you can have one task that uses a specific IAM role for access to S3 and one task that uses an IAM role to access DynamoDB With IAM roles for EC2 instances you assign all of the IAM policies required by tasks in the cluster to the EC2 instances that host the cluster. This does not allow the secure separation requested An instance profile is a container for an IAM role that you can use to pass role information to an EC2 instance when the instance starts. Again, this does not allow the secure separation requested Network ACLs are applied at the subnet level and would not assist here References: https://aws.amazon.com/blogs/compute/help-secure-container-enabled-applications-with-iam-roles-for-ecs-tasks/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

⚪ IAM Instance Profile for EC2 instances

⚪ Network ACLs

⚪ IAM roles for EC2 instances

Q34)

You are a Solutions Architect at Digital Cloud Training. One of your clients has a global presence and their web application runs out of multiple AWS regions. The client wants to personalize the experience for the customers in different parts of the world so they receive a customized application interface in the users' language. The client has created the customized web applications and need to ensure customers are directed to the correct application based on their location.

How can this be achieved?

⚪ Use Route 53 with a multi-value answer routing policy that presents multiple options to the users

⚪ Use CloudFront to cache the content in edge locations

✅ Use Route 53 with a geolocation routing policy that directs users based on their geographical location

Explanation:-Latency based routing would direct users to the closest region but geolocation allows you to configure settings based on specified attributes rather than just latency (distance) Geolocation provides: - Caters to different users in different countries and different languages - Contains users within a particular geography and offers them a customized version of the workload based on their specific needs - Geolocation can be used for localizing content and presenting some or all of your website in the language of your users - Can also protect distribution rights Multi-value answers are used for responding to DNS queries with up to eight healthy records selected at random CloudFront can cache content but would not provide the personalization features requested References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

⚪ Use Route 53 with a latency based routing policy that will direct users to the closest region

---

Q35)

You are running a database on an EC2 instance in your VPC. The load on the DB is increasing and you have noticed that the performance has been impacted.

Which of the options below would help to increase storage performance? (choose 2)

✅ Use EBS optimized instances

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

⚪ Use HDD, Cold (SC1) EBS volumes

⚪ Use a larger instance size within the instance family

✅ Use Provisioned IOPS (I01) EBS volumes

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

Q36)

An application you manage uses RDS in a multi-AZ configuration as the database back-end. There is a failure of the primary DB instance.

Which of the following statements are correct in relation to the process RDS uses to failover to the standby DB instance? (choose 2)

✅ Failover times are typically 60-120 seconds

Explanation:-The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance. As a result, you need to re-establish any existing connections to your DB instance The time it takes for the failover to complete depends on the database activity and other conditions at the time the primary DB instance became unavailable. Failover times are typically 60-120 seconds Multi-AZ does use synchronous replication but failover is not instantaneous The DN record is updated, not the IP address References: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

✅ The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance

Explanation:-The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance. As a result, you need to re-establish any existing connections to your DB instance The time it takes for the failover to complete depends on the database activity and other conditions at the time the primary DB instance became unavailable. Failover times are typically 60-120 seconds Multi-AZ does use synchronous replication but failover is not instantaneous The DN record is updated, not the IP address References: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

⚪ The failover mechanism automatically moves the Elastic IP address of the instance to the standby DB instance

⚪ Multi-AZ uses synchronous replication; therefore, the failover is instantaneous

---

Q37)

You have associated a new launch configuration to your Auto Scaling Group (ASG) which runs a fleet of EC2 instances. The new launch configuration changes monitoring from detailed to basic. There are a couple of CloudWatch alarms configured on the ASG which monitor every 60 seconds.

There is a mismatch in frequency of metric reporting between these configuration settings, what will be the result?

⚪ The EC2 metrics will be updated automatically to match the frequency of the alarms and send updates every 60 seconds

⚪ The ASG will automatically update the frequency of the alarms to 300 seconds to match the EC2 monitoring in the launch configuration

⚪ The alarm state will be immediately set to INSUFFICIENT_DATA

✅ If you do not update your alarms to match the five-minute period, they continue to check for statistics every minute and might find no data available for as many as four out of every five periods

Explanation:-If you have an Auto Scaling group and need to change which type of monitoring is enabled for your Auto Scaling instances, you must create a new launch configuration and update the Auto Scaling group to use this launch configuration. After that, the instances that the Auto Scaling group launches will use the updated monitoring type If you have CloudWatch alarms associated with your Auto Scaling group, use the put-metric-alarm command to update each alarm so that its period matches the monitoring type (300 seconds for basic monitoring and 60 seconds for detailed monitoring). If you change from detailed monitoring to basic monitoring but do not update your alarms to match the five-minute period, they continue to check for statistics every minute and might find no data available for as many as four out of every five periods References: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-monitoring.html#as-group-metrics

---

Q38)

You are 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 you are concerned about right-sizing the database.

What methods of scaling are possible after the MySQL RDS database is deployed? (choose 2)

✅ Vertical scaling for read and write by choosing a larger instance size

Explanation:-Relational databases can scale vertically (e.g. upgrading to a larger RDS DB instance) For read-heavy use cases, you can scale horizontally using read replicas There is no such thing as a Multi-Master MySQL RDS DB (there is for Aurora) You cannot scale write capacity by

enabling Multi-AZ as only one DB is active and can be written to Transfer Acceleration is a feature of S3 for fast uploads of objects References: https://aws.amazon.com/architecture/well-architected/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

✅ Horizontal scaling for read capacity by creating a read-replica

Explanation:-Relational databases can scale vertically (e.g. upgrading to a larger RDS DB instance) For read-heavy use cases, you can scale horizontally using read replicas There is no such thing as a Multi-Master MySQL RDS DB (there is for Aurora) You cannot scale write capacity by enabling Multi-AZ as only one DB is active and can be written to Transfer Acceleration is a feature of S3 for fast uploads of objects References: https://aws.amazon.com/architecture/well-architected/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- Horizontal scaling for read and write by enabling Multi-Master RDS DB
- Horizontal scaling for write capacity by enabling Multi-AZ

Q39)

When using the MySQL database with AWS RDS, features such as Point-In-Time restore and snapshot restore require a recoverable storage engine.

Which storage engine must be used to enable these features?

✅ InnoDB

Explanation:-RDS fully supports the InnoDB storage engine for MySQL DB instances. RDS features such as Point-In-Time restore and snapshot restore require a recoverable storage engine and are supported for the InnoDB storage engine only Automated backups and snapshots are not supported for MyISAM There is no storage engine called "memory" or "federated" References: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_MySQL.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- Federated
- MyISAM
- Memory

Q40)

One of your clients is transitioning their web presence into the AWS cloud. As part of the migration the client 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 you use to distribute traffic as requested?

- Use an Application Load Balancer to distribute traffic based on IP address
- Use Route 53 with a simple routing policy
- Use a Network Load Balancer to distribute traffic based on Instance ID

✅ Use Route 53 with a weighted routing policy and configure the respective weights

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 Network Load Balancer can distribute traffic to AWS and on-premise resources using IP addresses (not Instance IDs) 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 References: 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/

Q41) You are creating an operational dashboard in CloudWatch for a number of EC2 instances running in your VPC. Which one of the following metrics will not be available by default?

- Disk read operations
- Network in and out
- CPU utilization

✅ Memory usage

Explanation:-ul> There is no standard metric for memory usage on EC2 instances. Use the AWS website link below for a comprehensive list of the metrics that are collected References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/ https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ec2-metricscollected.html

---

Q42)

An application you manage uses and Elastic Load Balancer (ELB) and you need to enable session affinity. You are using the Application Load Balancer type and need to understand how the sticky sessions feature works.

Which of the statements below are correct in relation to sticky sessions? (choose 2)

✅ ALB supports load balancer-generated cookies only

Explanation:-The Application Load Balancer supports load balancer-generated cookies only (not application-generated) and the cookie name is always AWSALB. Sticky session are enabled at the target group level Session stickiness uses cookies and ensures a client is bound to an individual back-end instance for the duration of the cookie lifetime With ELB-inserted cookies if the back-end instance becomes unhealthy, new requests will be routed by the load balancer normally BUT the session will no longer be sticky References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

✅ Sticky sessions are enabled at the target group level

Explanation:-The Application Load Balancer supports load balancer-generated cookies only (not application-generated) and the cookie name is always AWSALB. Sticky session are enabled at the target group level Session stickiness uses cookies and ensures a client is bound to an individual back-end instance for the duration of the cookie lifetime With ELB-inserted cookies if the back-end instance becomes unhealthy, new requests will be routed by the load balancer normally BUT the session will no longer be sticky References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- Cookies can be inserted by the application or by the load balancer when configured

The name of the cookie is AWSSTICKY

Q43)

The security team in your company is defining new policies for enabling security analysis, resource change tracking, and compliance auditing. They would like to gain visibility into user activity by recording API calls made within the company's AWS account.

The information that is logged must be encrypted.

This requirement applies to all AWS regions in which your company has services running.

How will you implement this request? (choose 2)

✅ Create a CloudTrail trail and apply it to all regions

Explanation:-CloudTrail is used for recording API calls (auditing) whereas CloudWatch is used for recording metrics (performance monitoring). The solution can be deployed with a single trail that is applied to all regions. A single KMS key can be used to encrypt log files for trails applied to all regions. CloudTrail log files are encrypted using S3 Server Side Encryption (SSE) and you can also enable encryption SSE KMS for additional security You do not need to create a separate trail in each region or use multiple KMS keys CloudWatch is not used for monitoring API calls References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudtrail/

Use CloudWatch to monitor API calls

✅ Enable encryption with a single KMS key

Explanation:-CloudTrail is used for recording API calls (auditing) whereas CloudWatch is used for recording metrics (performance monitoring). The solution can be deployed with a single trail that is applied to all regions. A single KMS key can be used to encrypt log files for trails applied to all regions. CloudTrail log files are encrypted using S3 Server Side Encryption (SSE) and you can also enable encryption SSE KMS for additional security You do not need to create a separate trail in each region or use multiple KMS keys CloudWatch is not used for monitoring API calls References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudtrail/

Create a CloudTrail trail in each region in which you have services

---

Q44)

You are a Solutions Architect at Digital Cloud Training and you're reviewing a customer's design for a two-tier application with a stateless web front-end running on EC2 and a database back-end running on DynamoDB. The current design consists of a single EC2 web server that connects to the DynamoDB table to store session state data.The customer has requested that the data is stored across multiple physically separate locations for high availability and durability and the web front-end should be fault tolerant and able to scale automatically in times of high load.

What changes will you recommend to the client? (choose 2)

Add another compute in another Availability Zone and use Route 53 to distribute traffic using Round Robin

✅ Setup an Auto Scaling Group across multiple Availability Zones configured to run multiple EC2 instances across zones and use simple scaling to increase the group size during periods of high utilization

Explanation:-Availability Zones are physically separate and isolated from each other and you can use Auto Scaling to launch instances into multiple AZs within a region. This along with an ELB to distribute incoming connections between the instances in each AZ will provide the required fault tolerance. Amazon DynamoDB stores three geographically distributed replicas of each table to enable high availability and data durability so the session state data is already highly available and durable Adding another compute node in another AZ and using Route 53 round robin to distributed incoming connections may work but wouldn't provide the required ability to scale automatically in times of high load. This is where Auto Scaling and ELB can assist RDS is not used for storing session state data Elasticache Memcached cannot be used as a persistent datastore and does not support replication across AZs References: 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-dynamodb/

✅ Launch an Elastic Load Balancer and attach it to the Auto Scaling Group

Explanation:-Availability Zones are physically separate and isolated from each other and you can use Auto Scaling to launch instances into multiple AZs within a region. This along with an ELB to distribute incoming connections between the instances in each AZ will provide the required fault tolerance. Amazon DynamoDB stores three geographically distributed replicas of each table to enable high availability and data durability so the session state data is already highly available and durable Adding another compute node in another AZ and using Route 53 round robin to distributed incoming connections may work but wouldn't provide the required ability to scale automatically in times of high load. This is where Auto Scaling and ELB can assist RDS is not used for storing session state data Elasticache Memcached cannot be used as a persistent datastore and does not support replication across AZs References: 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-dynamodb/

Use RDS database in a Multi-AZ configuration to add high availability

---

Q45)

You work as an Enterprise Architect for Digital Cloud Training which employs 1500 people. The company is growing at around 5% per annum. The company strategy is to increasingly adopt AWS cloud services. There is an existing Microsoft Active Directory (AD) service that is used as the on-premise identity and access management system.

You want to avoid synchronizing your directory into the AWS cloud or adding permissions to resources in another AD domain.

Launch an AWS Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain

✅ Launch a large AWS Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication

Explanation:-The important points here are that you need to utilize the on-premise AD for authentication with AWS services whilst not synchronizing the AD database into the cloud or setting up trust relationships(adding permissions to resources in another AD domain). AD Connector is a directory gateway for redirecting directory requests to your on-premise Active Directory and eliminates the need for directory synchronization. AD connector is considered the best choice when you want to use an existing AD with AWS services. The small AD connector is for up to 500 users and the large version caters for up to 5000 so in this case we need to use the large AD connector Active Directory Service for Microsoft Active Directory is the best choice if you have more than 5000 users and is a standalone AD service in the cloud. You can also setup trust relationships with existing on-premise AD instances (though you can't replicate/synchronize). In this case we want to leverage the on-premise AD and want to avoid trust relationships The AWS Simple AD is an Active Directory compatible directory service in the cloud - it cannot be used to proxy authentication requests to the on-premise AD References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

- Install a Microsoft Active Directory Domain Controller on AWS and add it into your existing on-premise domain
- Use a large AWS Simple AD in AWS

Q46)

As a Solutions Architect at Digital Cloud Training you are helping a client to design a multi-tier web application architecture. The client has requested that the architecture provide low-latency connectivity between all servers and be resilient across multiple locations. They would also like to use their existing Microsoft SQL licenses for the database tier. The client needs to maintain the ability to access the operating systems of all servers for the installation of monitoring software.

How would you recommend the database tier is deployed?

- Amazon RDS with Microsoft SQL Server in a Multi-AZ configuration
- ✅ Amazon EC2 instances with Microsoft SQL Server and data replication between two different AZs

Explanation:-As the client needs to access the operating system of the database servers, we need to use EC2 instances not RDS (which does not allow operating system access). We can implement EC2 instances with Microsoft SQL in two different AZs which provides the requested location redundancy and AZs are connected by low-latency, high throughput and redundant networking Implementing the solution in a single AZ would not provide the resiliency requested RDS is a fully managed service and you do not have access to the underlying EC2 instance (no root access) References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- Amazon EC2 instances with Microsoft SQL Server and data replication within an AZ
- Amazon RDS with Microsoft SQL Server

Q47) A mobile client requires data from several application-layer services to populate its user interface. What can the application team use to decouple the client interface from the underlying services behind them?

- Application Load Balancer
- ✅ Amazon API Gateway

Explanation:-Amazon API Gateway decouples the client application from the back-end application-layer services by providing a single endpoint for API requetss An application load balancer distributes incoming connection requests to back-end EC2 instances. It is not used for decoupling application-layer services from mobile clients Amazon Cognito is used for adding sign-up, sign-in and access control to mobile apps AWS Device farm is an app testing service for Android, iOS and web apps References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

- Amazon Cognito
- AWS Device Farm

Q48)

A member of the security team in your organization has brought an issue to your attention. External monitoring tools have noticed some suspicious traffic coming from a small number of identified public IP addresses. The traffic is destined for multiple resources in your VPC.

What would be the easiest way to temporarily block traffic from the IP addresses to any resources in your VPC?

- Add a rule in the VPC route table that denies access to the VPC from the identified IP addresses
- ✅ Add a rule to the Network ACL to deny traffic from the identified IP addresses. Ensure all subnets are associated with the Network ACL

Explanation:-The best way to handle this situation is to create a deny rule in a network ACL using the identified IP addresses as the source. You would apply the network ACL to the subnet(s) that are seeing suspicious traffic You cannot create a deny rule with a security group You cannot use the route table to create security rules NAT Gateways are used for allowing instances in private subnets to access the Internet, they do not provide any inbound services References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Add a rule in each Security Group that is associated with the affected resources that denies traffic from the identified IP addresses
- Configure the NAT Gateway to deny traffic from the identified IP addresses

---

Q49)

A customer runs an API on their website that receives around 1,000 requests each day and has an average response time of 50 ms. It is currently hosted on a single c4.large EC2 instance.

How can high availability be added to the architecture at the LOWEST cost?

- Create an Auto Scaling group with a minimum of one instance and a maximum of two instances, then use an Application Load Balancer to balance the traffic
- Recreate the API using API Gateway and integrate the API with the existing back-end
- Create an Auto Scaling group with a maximum of two instances, then use an Application Load Balancer to balance the traffic
- ✅ Recreate the API using API Gateway and use AWS Lambda as the service back-end

Explanation:-The API does not receive a high volume of traffic or require extremely low latency. It would not be cost efficient to use multiple EC2 instances and Elastic Load Balancers. Instead the best course of action would be to recreate the API using API Gateway which will allow the customer to only pay for what they use. AWS Lambda can likewise be used for the back-end processing reducing cost by utilizing a pay for what you use serverless service If the architect recreates the API using API Gateway but integrates the API with the existing back-end this is not highly available and is not the lowest cost option Using Application Load Balancers with multiple EC2 instances would not be cost effective References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/

Q50)

You would like to grant additional permissions to an individual ECS application container on an ECS cluster that you have deployed. You would like to do this without granting additional permissions to the other containers that are running on the cluster.

How can you achieve this?

✅ Create a separate Task Definition for the application container that uses a different Task Role

Explanation:-You can only apply one IAM role to a Task Definition so you must create a separate Task Definition.. A Task Definition is required to run Docker containers in Amazon ECS and you can specify the IAM role (Task Role) that the task should use for permissions It is incorrect to say that you cannot implement granular permissions with ECS containers as IAM roles are granular and are applied through Task Definitions/Task Roles You can apply different IAM roles to different EC2 instances, but to grant permissions to ECS application containers you must use Task Definitions and Task Roles References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

- In the same Task Definition, specify a separate Task Role for the application container
- Use EC2 instances instead as you can assign different IAM roles on each instance
- You cannot implement granular permissions with ECS containers