Answer Sheet

Q1)

A Solutions Architect is designing the system monitoring and deployment layers of a serverless application. The system monitoring layer will manage system visibility through recording logs and metrics and the deployment layer will deploy the application stack and manage workload changes through a release management process.The Architect needs to select the most appropriate AWS services for these functions.

Which services and frameworks should be used for the system monitoring and deployment layers? (choose 2)

- Use AWS X-Ray to package, test, and deploy the serverless application stack
- ✅ Use AWS SAM to package, test, and deploy the serverless application stack

Explanation:-AWS Serverless Application Model (AWS SAM) is an extension of AWS CloudFormation that is used to package, test, and deploy serverless applications With Amazon CloudWatch, you can access system metrics on all the AWS services you use, consolidate system and application level logs, and create business key performance indicators (KPIs) as custom metrics for your specific needs AWS Lambda is used for executing your code as functions, it is not used for packaging, testing and deployment. AWS Lambda is used with AWS SAM AWS X-Ray lets you analyze and debug serverless applications by providing distributed tracing and service maps to easily identify performance bottlenecks by visualizing a request end-to-end References: https://docs.aws.amazon.com/lambda/latest/dg/serverless_app.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/

- Use AWS Lambda to package, test, and deploy the serverless application stack
- ✅ Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics

Explanation:-AWS Serverless Application Model (AWS SAM) is an extension of AWS CloudFormation that is used to package, test, and deploy serverless applications With Amazon CloudWatch, you can access system metrics on all the AWS services you use, consolidate system and application level logs, and create business key performance indicators (KPIs) as custom metrics for your specific needs AWS Lambda is used for executing your code as functions, it is not used for packaging, testing and deployment. AWS Lambda is used with AWS SAM AWS X-Ray lets you analyze and debug serverless applications by providing distributed tracing and service maps to easily identify performance bottlenecks by visualizing a request end-to-end References: https://docs.aws.amazon.com/lambda/latest/dg/serverless_app.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/

Q2) You have just created a new security group in your VPC. You have not yet created any rules. Which of the statements below are correct regarding the default state of the security group? (choose 2)

- There is an outbound rule allowing traffic to the Internet Gateway
- ✅ There is an outbound rule that allows all traffic to all IP addresses

Explanation:-Custom security groups do not have inbound allow rules (all inbound traffic is denied by default) Default security groups do have inbound allow rules (allowing traffic from within the group) All outbound traffic is allowed by default in both custom and default security groups Security groups act like a stateful firewall at the instance level. Specifically security groups operate at the network interface level of an EC2 instance. You can only assign permit rules in a security group, you cannot assign deny rules and there is an implicit deny rule at the end of the security group. All rules are evaluated until a permit is encountered or continues until the implicit deny. You can create ingress and egress rules. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- ✅ There are no inbound rules and traffic will be implicitly denied

Explanation:-Custom security groups do not have inbound allow rules (all inbound traffic is denied by default) Default security groups do have inbound allow rules (allowing traffic from within the group) All outbound traffic is allowed by default in both custom and default security groups Security groups act like a stateful firewall at the instance level. Specifically security groups operate at the network interface level of an EC2 instance. You can only assign permit rules in a security group, you cannot assign deny rules and there is an implicit deny rule at the end of the security group. All rules are evaluated until a permit is encountered or continues until the implicit deny. You can create ingress and egress rules References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- There are is an inbound rule that allows traffic from the Internet Gateway

---

Q3)

You need to setup a distribution method for some static files. The requests will be mainly GET requests and you are expecting a high volume of GETs often exceeding 2000 per second. The files are currently stored in an S3 bucket.

According to AWS best practices, what can you do to optimize performance?

- Use S3 Transfer Acceleration
- Use ElastiCache to cache the content
- ✅ Integrate CloudFront with S3 to cache the content

Explanation:-Amazon S3 automatically scales to high request rates. For example, your application can achieve at least 3,500 PUT/POST/DELETE and 5,500 GET requests per second per prefix in a bucket. There are no limits to the number of prefixes in a bucket If your workload is mainly sending GET requests, in addition to the preceding guidelines, you should consider using Amazon CloudFront for performance optimization. By integrating CloudFront with Amazon S3, you can distribute content to your users with low latency and a high data transfer rate Transfer Acceleration is used to accelerate object uploads to S3 over long distances (latency) Cross-region replication creates a replica copy in another region but should not be used for spreading read requests across regions. There will be 2 S3 endpoints and CRR is not designed for 2 way sync so this would not work well ElastiCache is used for caching database content not S3 content References: https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Use cross-region replication to spread the load across regions

---

Q4)

Your company has started using the AWS CloudHSM for secure key storage. A recent administrative error resulted in the loss of credentials to access the CloudHSM. You need access to data that was encrypted using keys stored on the hardware security module.

How can you recover the keys that are no longer accessible?

- Log a case with AWS support and they will use MFA to recover the credentials

✅ There is no way to recover your keys if you lose your credentials

Explanation:-Amazon does not have access to your keys or credentials and therefore has no way to recover your keys if you lose your credentials. References: https://aws.amazon.com/cloudhsm/faqs/

- Restore a snapshot of the CloudHSM
- Reset the CloudHSM device and create a new set of credentials

---

Q5)

You have implemented the AWS Elastic File System (EFS) to store data that will be accessed by a large number of EC2 instances. The data is sensitive and you are working on a design for implementing security measures to protect the data. You need to ensure that network traffic is restricted correctly based on firewall rules and access from hosts is restricted by user or group.

How can this be achieved with EFS? (choose 2)

- Use AWS Web Application Firewall (WAF) to protect EFS
- ✅ Use POSIX permissions to control access from hosts by user or group

Explanation:-You can control who can administer your file system using IAM. You can control access to files and directories with POSIX-compliant user and group-level permissions. POSIX permissions allows you to restrict access from hosts by user and group. EFS Security Groups act as a firewall, and the rules you add define the traffic flow You cannot use AWS WAF to protect EFS data using users and groups You do not use IAM to control access to files and directories by user and group, but you can use IAM to control who can administer the file system configuration You use EFS Security Groups to control network traffic to EFS, not Network ACLs References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/ https://aws.amazon.com/efs/features/

- Use Network ACLs to control the traffic
- ✅ Use EFS Security Groups to control network traffic

Explanation:-You can control who can administer your file system using IAM. You can control access to files and directories with POSIX-compliant user and group-level permissions. POSIX permissions allows you to restrict access from hosts by user and group. EFS Security Groups act as a firewall, and the rules you add define the traffic flow You cannot use AWS WAF to protect EFS data using users and groups You do not use IAM to control access to files and directories by user and group, but you can use IAM to control who can administer the file system configuration You use EFS Security Groups to control network traffic to EFS, not Network ACLs References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/ https://aws.amazon.com/efs/features/

Q6)

You have recently enabled Access Logs on your Application Load Balancer (ALB). One of your colleagues would like to process the log files using a hosted Hadoop service.

What configuration changes and services can be leveraged to deliver this requirement?

- Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files
- Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files
- Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files
- ✅ Configure Access Logs to be delivered to S3 and use EMR for processing the log files

Explanation:-Access Logs can be enabled on ALB and configured to store data in an S3 bucket. Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3 Neither Kinesis or EC2 provide a hosted Hadoop service You cannot configure access logs to be delivered to DynamoDB References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q7)

You are designing the disk configuration for an EC2 instance. The instance needs to support a MapReduce process that requires high throughput for a large dataset with large I/O sizes. You need to provision the most cost-effective storage solution option.

What EBS volume type will you select?

- EBS General Purpose SSD
- EBS Provisioned IOPS SSD
- EBS General Purpose SSD in a RAID 1 configuration
- ✅ EBS Throughput Optimized HDD

Explanation:-EBS Throughput Optimized HDD is good for the following use cases (and is the most cost-effective option: Frequently accessed, throughput intensive workloads with large datasets and large I/O sizes, such as MapReduce, Kafka, log processing, data warehouse, and ETL workloads Throughput is measured in MB/s, and includes the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume The SSD options are more expensive References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

Q8)

An EC2 instance you manage is generating very high packets-per-second and performance of the application stack is being impacted. You have been asked for a resolution to the issue that results in improved performance from the EC2 instance.

What would you suggest?

- Create a placement group and put the EC2 instance in it
- Add multiple Elastic IP addresses to the instance
- ✅ Use enhanced networking

Explanation:-Enhanced networking provides higher bandwidth, higher packet-per-second (PPS) performance, and consistently lower inter-instance latencies. If your packets-per-second rate appears to have reached its ceiling, you should consider moving to enhanced networking because you have likely reached the upper thresholds of the VIF driver. It is only available for certain instance types and only supported in VPC. You must also

launch an HVM AMI with the appropriate drivers AWS currently supports enhanced networking capabilities using SR-IOV. SR-IOV provides direct access to network adapters, provides higher performance (packets-per-second) and lower latency You do not need to create a RAID 1 array (which is more for redundancy than performance anyway) A placement group is used to increase network performance between instances. In this case there is only a single instance so it won't help Adding multiple IP addresses is not a way to increase performance of the instance as the same amount of bandwidth is available to the Elastic Network Interface (ENI). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/

- Configure a RAID 1 array from multiple EBS volumes

Q9)

A web application you manage receives order processing information from customers and places the messages on an SQS queue. A fleet of EC2 instances are configured to pick up the messages, process them, and store the results in a DynamoDB table. The current configuration has been resulting in a large number of empty responses to ReceiveMessage requests.

You would like to update the configuration to eliminate empty responses to reduce operational overhead. How can this be done?

- Configure Short Polling to eliminate empty responses by reducing the length of time a connection request remains open
- Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received
- Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once
- ✅ Configure Long Polling to eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response

Explanation:-The correct answer is to use Long Polling which will eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response The problem does not relate to the order in which the messages are processed in and there are no concerns over messages being delivered more than once so it doesn't matter whether you use a FIFO or standard queue Long Polling: - Uses fewer requests and reduces cost - Eliminates false empty responses by querying all servers - SQS waits until a message is available in the queue before sending a response - Requests contain at least one of the available messages up to the maximum number of messages specified in the ReceiveMessage action - Shouldn't be used if your application expects an immediate response to receive message calls - ReceiveMessageWaitTime is set to a non-zero value (up to 20 seconds) - Same charge per million requests as short polling Changing the queue type would not assist in this situation Short Polling: - Does not wait for messages to appear in the queue - It queries only a subset of the available servers for messages (based on weighted random execution) - Short polling is the default - ReceiveMessageWaitTime is set to 0 - More requests are used, which implies higher cost References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/ https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-long-polling.html

---

Q10)

You are running an Auto Scaling Group (ASG) with an Elastic Load Balancer (ELB) and a fleet of EC2 instances. Health checks are configured on the ASG to use EC2 status checks The ELB has determined that an EC2 instance is unhealthy and has removed it from service. However, you noticed that the instance is still running and has not been terminated by the ASG.

What would be an explanation for this?

- Connection draining is enabled and the ASG is waiting for in-flight requests to complete
- The health check grace period has not yet expired
- The ASG is waiting for the cooldown timer to expire before terminating the instance
- ✅ The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service

Explanation:-If using an ELB it is best to enable ELB health checks as otherwise EC2 status checks may show an instance as being healthy that the ELB has determined is unhealthy. In this case the instance will be removed from service by the ELB but will not be terminated by Auto Scaling Connection draining is not the correct answer as the ELB has taken the instance out of service so there are no active connections The health check grace period allows a period of time for a new instance to warm up before performing a health check More information on ASG health checks: By default uses EC2 status checks Can also use ELB health checks and custom health checks ELB health checks are in addition to the EC2 status checks If any health check returns an unhealthy status the instance will be terminated With ELB an instance is marked as unhealthy if ELB reports it as OutOfService A healthy instance enters the InService state If an instance is marked as unhealthy it will be scheduled for replacement If connection draining is enabled, Auto Scaling waits for in-flight requests to complete or timeout before terminating instances The health check grace period allows a period of time for a new instance to warm up before performing a health check (300 seconds by default) References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

Q11)

Your company runs a web-based application that uses EC2 instances for the web front-end and RDS for the database back-end. The web application writes transaction log files to an S3 bucket and the quantity of files is becoming quite large. You have determined that it is acceptable to retain the most recent 60 days of log files and permanently delete the rest.

What can you do to enable this to happen automatically?

- ✅ Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old

Explanation:-Moving logs to Glacier may save cost but the questions requests that the files are permanently deleted Object Expiration allows you to schedule removal of your objects after a defined time period Using Object Expiration rules to schedule periodic removal of objects eliminates the need to build processes to identify objects for deletion and submit delete requests to Amazon S3 References: https://aws.amazon.com/about-aws/whats-new/2011/12/27/amazon-s3-announces-object-expiration/ https://aws.amazon.com/about-aws/whats-new/2011/12/27/amazon-s3-announces-object-expiration/

- Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old
- Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class
- Use an S3 bucket policy that deletes objects that are more than 60 days old

---

Q12)

A DynamoDB table you manage has a variable load, ranging from sustained heavy usage some days, to only having small spikes on others. The load is 80% read and 20% write. The provisioned throughput capacity has been configured to account for the heavy load to ensure throttling does not occur.You have been asked to find a solution for saving cost.

What would be the most efficient and cost-effective solution?

- Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput
- ✅ Create a DynamoDB Auto Scaling scaling policy

Explanation:-DynamoDB auto scalinguses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This is the most efficient and cost-effective solution Manually adjusting the provisioned throughput is not efficient Using AWS Lambda to modify the provisioned throughput is possible but it would be more cost-effective to use DynamoDB Auto Scaling as there is no cost to using it DynamoDB DAX is an in-memory cache that increases the performance of DynamoDB. However, it costs money and there is no requirement to increase performance References: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

- Use DynamoDB DAX to increase the performance of the database
- Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput

---

Q13)

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. The client uses Microsoft SQL Server for existing databases.

The client has a limited budget for staff costs and does not need to access the underlying operating system

What would you recommend as the most efficient solution?

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

Explanation:-As the client does not need to manage the underlying operating system and they have a limited budget for staff, they should use a managed service such as RDS. Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it which enables the required resilience across multiple locations With EC2 you have full control at the operating system layer (not required) and can install your own database. However, you would then need to manage the entire stack and therefore staff costs would increase so this is not the best solution. 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/

Q14)

An organization in the agriculture sector is deploying sensors and smart devices around factory plants and fields. The devices will collect information and send it to cloud applications running on AWS.

Which AWS service will securely connect the devices to the cloud applications?

- AWS DMS
- AWS Glue
- AWS Lambda
- ✅ AWS IoT Core

Explanation:-An organization in the agriculture sector is deploying sensors and smart devices around factory plants and fields. The devices will collect information and send it to cloud applications running on AWS

Q15)

A development team needs to run up a few lab servers on a weekend for a new project. The servers will need to run uninterrupted for a few hours.

Which EC2 pricing option would be most suitable?

- Dedicated instances
- ✅ On-Demand

Explanation:-Spot pricing may be the most economical option for a short duration over a weekend but you may have the instances terminated by AWS and there is a requirement that the servers run uninterrupted On-Demand pricing ensures that instances will not be terminated and is the most economical option Reserved pricing provides a reduced cost for a contracted period (1 or 3 years), and is not suitable for ad hoc requirements Dedicated instances run on hardware that's dedicated to a single customer and are more expensive than regular On-Demand instances References: https://aws.amazon.com/ec2/pricing/

- Reserved
- Spot

Q16)

A security officer has requested that all data associated with a specific customer is encrypted. The data resides on Elastic Block Store (EBS) volumes.

Which of the following statements about using EBS encryption are correct? (choose 2)

- ✅ There is no direct way to change the encryption state of a volume

Explanation:-All EBS types and all instance families support encryption Not all instance types support encryption There is no direct way to change the encryption state of a volume Data in transit between an instance and an encrypted volume is also encrypted You can have encrypted and non-encrypted EBS volumes on a single instance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

- All instance types support encryption
- All attached EBS volumes must share the same encryption state
- ✅ Data in transit between an instance and an encrypted volume is also encrypted

Explanation:-All EBS types and all instance families support encryption Not all instance types support encryption There is no direct way to change the encryption state of a volume Data in transit between an instance and an encrypted volume is also encrypted You can have encrypted and non-encrypted EBS volumes on a single instance. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

Q17)

You are putting together an architecture for a new VPC on AWS. Your on-premise data center will be connected to the VPC by a hardware VPN and has public and VPN-only subnets.

The security team has requested that all traffic that hits the public subnets on AWS must be directed over the VPN to the corporate firewall. How can this be achieved?

- In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway
- Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway
- In the public subnet route table, add a route for your remote network and specify the customer gateway as the target
- ✅ In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target

Explanation:-Route tables determine where network traffic is directed. In your route table, you must add a route for your remote network and specify the virtual private gateway as the target. This enables traffic from your VPC that's destined for your remote network to route via the virtual private gateway and over one of the VPN tunnels. You can enable route propagation for your route table to automatically propagate your network routes to the table for you You must select the virtual private gateway (AWS side of the VPN) not the customer gateway (customer side of the VPN) in the target in the route table NAT Gateways are used to enable Internet access for EC2 instances in private subnets, they cannot be used to direct traffic to VPG You must create the route table rule in the route table attached to the public subnet, not the VPN-only subnet References: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_VPN.html

---

Q18)

One of your clients has requested advice on the correct choice of Elastic Load Balancer (ELB) for an application they are planning to deploy on AWS. The application requires extremely high throughput and extremely low latencies. The connections will be made using the TCP protocol and the ELB must support load balancing to multiple ports on an instance.

Which ELB would you suggest the client uses?

- ✅ Network Load Balancer

Explanation:-The Network Load Balancer operates at the connection level (Layer 4), routing connections to targets – Amazon EC2 instances, containers and IP addresses based on IP protocol data. It is architected to handle millions of requests/sec, sudden volatile traffic patterns and provides extremely low latencies. It provides high throughput and extremely low latencies and is designed to handle traffic as it grows and can load balance millions of requests/second. NLB also supports load balancing to multiple ports on an instance The CLB operates using the TCP, SSL, HTTP and HTTPS protocols. It is not the best choice for requirements of extremely high throughput and low latency and does not support load balancing to multiple ports on an instance The ALB operates at the HTTP and HTTPS level only (does not support TCP load balancing) Route 53 is a DNS service, it is not a type of ELB (though you can do some types of load balancing with it) References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- Classic Load Balancer
- Application Load Balancer
- Route 53

Q19) An RDS database is experiencing heavy read traffic. You are planning on creating read replicas. When using Amazon RDS with Read Replicas, which of the deployment options below are valid? (choose 2)

- Cross-Continent
- ✅ Cross-Availability Zone

Explanation:-Read Replicas can be within an AZ, Cross-AZ and Cross-Region Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas are for workload sharing and offloading Read replicas cannot be cross-continent, cross-subnet or cross-facility. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- Cross-subnet
- ✅ Within an Availability Zone

Explanation:-Read Replicas can be within an AZ, Cross-AZ and Cross-Region Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas are for workload sharing and offloading Read replicas cannot be cross-continent, cross-subnet or cross-facility. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

Q20) A developer is writing code for AWS Lambda and is looking to automate the release process. Which AWS services can be used to automate the release process of Lambda applications? (choose 2)

- ✅ AWS CodePipeline

Explanation:-You can automate your serverless application's release process using AWS CodePipeline and AWS CodeDeploy The following AWS services can be used to fully automate the deployment process: You use CodePipeline to model, visualize, and automate the steps required to release your serverless application You use AWS CodeDeploy to gradually deploy updates to your serverless applications You use CodeBuild to build, locally test, and package your serverless application You use AWS CloudFormation to deploy your application References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/ https://docs.aws.amazon.com/lambda/latest/dg/build-pipeline.html

- AWS Glue
- AWS OpsWorks
- ✅ AWS CodeDeploy

Explanation:-You can automate your serverless application's release process using AWS CodePipeline and AWS CodeDeploy The following AWS services can be used to fully automate the deployment process: You use CodePipeline to model, visualize, and automate the steps required to release your serverless application You use AWS CodeDeploy to gradually deploy updates to your serverless applications You use CodeBuild to build, locally test, and package your serverless application You use AWS CloudFormation to deploy your application References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/ https://docs.aws.amazon.com/lambda/latest/dg/build-pipeline.html

Q21) In your VPC you have several EC2 instances that have been running for some time. You have logged into an instance and need to determine a few pieces of information including what IAM role is assigned, the instance ID and the names of the security groups that are assigned to the instance.From the options below, what would be a source of this information?

- Tags
- ✓ Metadata

Explanation:-Instance metadata is data about your instance that you can use to configure or manage the running instance and is available at http://169.254.169.254/latest/meta-data Tags are used to categorize and label resources Parameters are used in databases User data is used to configure the system at launch time and specify scripts. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html#instancedata-data-categories

- Parameters
- User data

Q22)

The application development team in your company have developed a Java application and saved the source code in a .war file. They would like to run the application on AWS resources and are looking for a service that can handle the provisioning and management of the underlying resources it will run on.

What AWS service would allow the developers to upload the Java source code file and provide capacity provisioning and infrastructure management?

- AWS CloudFormation
- AWS CodeDeploy
- AWS OpsWorks
- ✓ AWS Elastic Beanstalk

Explanation:-AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby, as well as different platform configurations for each language. To use Elastic Beanstalk, you create an application, upload an application version in the form of an application source bundle (for example, a Java .war file) to Elastic Beanstalk, and then provide some information about the application AWS CloudFormation uses templates to deploy infrastructure as code. It is not a PaaS service like Elastic Beanstalk and is more focussed on infrastructure than applications and management of applications AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/ https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html

---

Q23)

A development team are creating a Continuous Integration and Continuous Delivery (CI/CD) toolchain on the AWS cloud. The team currently use Jenkins X and Kubernetes on-premise and are looking to utilize the same services in the AWS cloud.

What AWS service can provide a managed container platform that is MOST similar to their current CI/CD toolchain?

- AWS CodePipeline
- Amazon ECS
- AWS Lambda
- ✓ Amazon EKS

Explanation:-Amazon EKS is AWS' managed Kubernetes offering, which enables you to focus on building applications, while letting AWS handle managing Kubernetes and the underlying cloud infrastructure Amazon Elastic Container Service (ECS) does not use Kubernetes so it is not the most similar product AWS Lambda is a serverless service that executes code as functions AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. It is not a container platform References: https://aws.amazon.com/eks/

Q24)

You are a Solutions Architect at Digital Cloud Training. One of your clients has requested some advice on how to implement security measures in their VPC. The client has recently been the victim of some hacking attempts. Fortunately, no data has been exposed at this point but the client wants to implement measures to mitigate further threats. The client has explained that the attacks always come from the same small block of IP addresses.

What would be a quick and easy measure to help prevent further attacks?

- ✓ Use a Network ACL rule that denies connections from the block of IP addresses

Explanation:-With NACLs you can have permit and deny rules. Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic With Security Groups you can only assign permit rules, you cannot assign deny rules A bastion host is typically used for admin purposes, allowing access to a single endpoint in the AWS cloud for administration using SSH/RDP. From the bastion instance you then connect to other EC2 instances in your subnets. This is not used as a method of adding security to production systems and cannot stop traffic from hitting application ports CloudFront does have DDoS prevention features but we don't know that this is a DDoS style of attack and CloudFront can only help where the traffic is using the CloudFront service to access cached content References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Use a Security Group rule that denies connections from the block of IP addresses
- Use CloudFront's DDoS prevention features
- Create a Bastion Host restrict all connections to the Bastion Host only

---

Q25)

A company is investigating ways to analyze and process large amounts of data in the cloud faster, without needing to load or transform the data in a data warehouse.

The data resides in Amazon S3.

Which AWS services would allow the company to query the data in place? (choose 2)

✅ Amazon RedShift Spectrum

Explanation:-Amazon S3 Select is designed to help analyze and process data within an object in Amazon S3 buckets, faster and cheaper. It works by providing the ability to retrieve a subset of data from an object in Amazon S3 using simple SQL expressions Amazon Redshift Spectrum allows you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. It does not allow you to perform query-in-place operations on S3 Amazon Elasticsearch Service, is a fully managed service that makes it easy for you to deploy, secure, operate, and scale Elasticsearch to search, analyze, and visualize data in real-time Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/ https://aws.amazon.com/blogs/aws/s3-glacier-select/ https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-redshift-spectrum-is-now-available-in-four-additional-aws-regions-and-enhances-query-performance-in-all-available-aws-regions/

✅ Amazon S3 Select

Explanation:-Amazon S3 Select is designed to help analyze and process data within an object in Amazon S3 buckets, faster and cheaper. It works by providing the ability to retrieve a subset of data from an object in Amazon S3 using simple SQL expressions Amazon Redshift Spectrum allows you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. It does not allow you to perform query-in-place operations on S3 Amazon Elasticsearch Service, is a fully managed service that makes it easy for you to deploy, secure, operate, and scale Elasticsearch to search, analyze, and visualize data in real-time Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/ https://aws.amazon.com/blogs/aws/s3-glacier-select/ https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-redshift-spectrum-is-now-available-in-four-additional-aws-regions-and-enhances-query-performance-in-all-available-aws-regions/

⬜ Amazon Kinesis Data Streams

⬜ Amazon Elasticsearch

Q26)

One of you clients has asked for assistance with a performance issue they are experiencing. The client has a fleet of EC2 instances behind an Elastic Load Balancer (ELB) that are a mixture of c4.2xlarge instance types and c5.large instances. The load on the CPUs on the c5.large instances has been very high, often hitting 100% utilization, whereas the c4.2xlarge instances have been performing well.

The client has asked for advice on the most cost effective way to resolve the performance problems?

⬜ Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances

⬜ Add more c5.large instances to spread the load more evenly

⬜ Add all of the instances into a Placement Group

✅ Change the configuration to use only c4.2xlarge instance types

Explanation:-The 2xlarge instance type provides more CPUs. The best answer is to use this instance type for all instances A placement group helps provide low-latency connectivity between instances and would not help here The weighted routing policy is a Route 53 feature that would not assist in this situation References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

Q27)

A company is deploying a new two-tier web application that uses EC2 web servers and a DynamoDB database backend. An Internet facing ELB distributes connections between the web servers.The Solutions Architect has created a security group for the web servers and needs to create a security group for the ELB.

What rules should be added? (choose 2)

⬜ Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway

✅ Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group

Explanation:-An inbound rule should be created for the relevant protocols (HTTP/HTTPS) and the source should be set to any address (0.0.0.0/0) The address 0.0.0.0/32 is incorrect as the 32 mask means an exact match is required (0.0.0.0) The outbound rule should forward the relevant protocols (HTTP/HTTPS) and the destination should be set to the web server security group Using the VPC CIDR would not be secure and you cannot specify an Internet Gateway in a security group (not that you'd want to anyway) FYI on the web server security group you'd want to add an Inbound rule allowing HTTP/HTTPS from the ELB security group References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

⬜ Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR

✅ Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0

Explanation:-An inbound rule should be created for the relevant protocols (HTTP/HTTPS) and the source should be set to any address (0.0.0.0/0) The address 0.0.0.0/32 is incorrect as the 32 mask means an exact match is required (0.0.0.0) The outbound rule should forward the relevant protocols (HTTP/HTTPS) and the destination should be set to the web server security group Using the VPC CIDR would not be secure and you cannot specify an Internet Gateway in a security group (not that you'd want to anyway) FYI on the web server security group you'd want to add an Inbound rule allowing HTTP/HTTPS from the ELB security group References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q28) You launched an EBS-backed EC2 instance into your VPC. A requirement has come up for some high-performance ephemeral storage and so you would like to add an instance-store backed volume. How can you add the new instance store volume?

✅ You can specify the instance store volumes for your instance only when you launch an instance

Explanation:-You can specify the instance store volumes for your instance only when you launch an instance. You can't attach instance store volumes to an instance after you've launched it You can use a block device mapping to specify additional EBS volumes when you launch your instance, or you can attach additional EBS volumes after your instance is running An Elastic Network Adapter has nothing to do with adding instance store volumes References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/add-instance-store-volumes.html

⬜ You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume

- You can use a block device mapping to specify additional instance store volumes when you launch your instance, or you can attach additional instance store volumes after your instance is running
- You must shutdown the instance in order to be able to add the instance store volume

---

Q29) You have just created a new Network ACL in your VPC. You have not yet created any rules. Which of the statements below are correct regarding the default state of the Network ACL? (choose 2)

- There is a default outbound rule allowing traffic to the Internet Gateway
- ✅ There is a default outbound rule denying all traffic

Explanation:-A VPC automatically comes with a default network ACL which allows all inbound/outbound traffic A custom NACL denies all traffic both inbound and outbound by default Network ACL's function at the subnet level and you can have permit and deny rules. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic. Network ACLs are stateless so responses are subject to the rules for the direction of traffic. NACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- There is a default inbound rule allowing traffic from the VPC CIDR block
- ✅ There is a default inbound rule denying all traffic

Explanation:-A VPC automatically comes with a default network ACL which allows all inbound/outbound traffic A custom NACL denies all traffic both inbound and outbound by default Network ACL's function at the subnet level and you can have permit and deny rules. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic. Network ACLs are stateless so responses are subject to the rules for the direction of traffic. NACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q30)

A large quantity of data that is rarely accessed is being archived onto Amazon Glacier. Your CIO wants to understand the resilience of the service.

Which of the statements below is correct about Amazon Glacier storage? (choose 2)

- Data is resilient in the event of one entire region destruction
- ✅ Provides 99.999999999% durability of archives

Explanation:-Glacier is designed for durability of 99.999999999% of objects across multiple Availability Zones. Data is resilient in the event of one entire Availability Zone destruction. Glacier supports SSL for data in transit and encryption of data at rest. Glacier is extremely low cost and is ideal for long-term archival Data is not resilient to the failure of an entire region Data is not replicated globally There is no availability SLA with Glacier References: https://aws.amazon.com/s3/storage-classes/

- Data is replicated globally
- ✅ Data is resilient in the event of one entire Availability Zone destruction

Explanation:-Glacier is designed for durability of 99.999999999% of objects across multiple Availability Zones. Data is resilient in the event of one entire Availability Zone destruction. Glacier supports SSL for data in transit and encryption of data at rest. Glacier is extremely low cost and is ideal for long-term archival Data is not resilient to the failure of an entire region Data is not replicated globally There is no availability SLA with Glacier References: https://aws.amazon.com/s3/storage-classes/

Q31)

You are planning to launch a fleet of EC2 instances running Linux. As part of the launch you would like to install some application development frameworks and custom software onto the instances. The installation will be initiated using some scripts you have written.

What feature allows you to specify the scripts so you can install the software during the EC2 instance launch?

- Run command
- ✅ User data

Explanation:-When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives User data is data that is supplied by the user at instance launch in the form of a script and is limited to 16KB User data and meta data are not encrypted. Instance metadata is available at http://169.254.169.254/latest/meta-data. The Instance Metadata Query tool allows you to query the instance metadata without having to type out the full URI or category names The AWS Systems Manager run command is used to manage the configuration of existing instances by using remotely executed commands. User data is better for specifying scripts to run at startup. References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

- AWS Config
- Metadata

Q32) One of your clients has multiple VPCs that are peered with each other. The client would like to use a single Elastic Load Balancer (ELB) to route traffic to multiple EC2 instances in peered VPCs within the same region. Is this possible?

- This is possible using the Classic Load Balancer (CLB) if using Instance IDs
- This is not possible with ELB, you would need to use Route 53
- No, the instances that an ELB routes traffic to must be in the same VPC
- ✅ This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets

Explanation:-With ALB and NLB IP addresses can be used to register: Instances in a peered VPC AWS resources that are addressable by IP address and port On-premises resources linked to AWS through Direct Connect or a VPN connection. References: https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q33)

One of the applications you manage receives a high traffic loads between 7:30am and 9:30am daily. The application uses an Auto Scaling Group (ASG) to maintain 3 EC2 instances most of the time but during the peak period requires 6 EC2 instances.

How can you configure ASG to perform a regular scale-out event at 7:30am and a scale-in event at 9:30am daily to account for the peak load?

- Use a Simple scaling policy
- ✅ Use a Scheduled scaling policy

Explanation:-Simple – maintains a current number of instances, you can manually change the ASGs min/desired/max and attach/detach instances Scheduled – Used for predictable load changes, can be a single event or a recurring schedule Dynamic (event based) – scale in response to an event/alarm Step – configure multiple scaling steps in response to multiple alarms References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- Use a Dynamic scaling policy
- Use a Step scaling policy

Q34)

An application is generating a large amount of clickstream events data that is being stored on S3. The business needs to understand customer behaviour and want to run complex analytics queries against the data.

Which AWS service can be used for this requirement?

- Amazon Kinesis Firehose
- ✅ Amazon 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 used for running complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution RDS is a relational database that is used for transactional workloads not analytics workloads Amazon Neptune is a new product that offers a fully-managed Graph database Amazon Kinesis Firehose processes streaming data, not data stored on S3. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

- Amazon RDS
- Amazon Neptune

Q35) One of your EC2 instances that is behind an Elastic Load Balancer (ELB) is in the process of being de-registered. Which ELB feature can be used to allow existing connections to close cleanly?

- Deletion Protection
- ✅ Connection Draining

Explanation:-Connection draining is enabled by default and provides a period of time for existing connections to close cleanly. When connection draining is in action an CLB will be in the status “InService: Instance deregistration currently in progress?? Session stickiness uses cookies and ensures a client is bound to an individual back-end instance for the duration of the cookie lifetime Deletion protection is used to protect the ELB from deletion The Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connections. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- Sticky Sessions
- Proxy Protocol

Q36)

You are a Solutions Architect at Digital Cloud Training. A large multi-national client has requested a design for a multi-region database. The master database will be in the EU (Frankfurt) region and databases will be located in 4 other regions to service local read traffic. The database should be a fully managed service including the replication.

Which AWS service can deliver these requirements?

- ✅ RDS with cross-region Read Replicas

Explanation:-RDS Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas are for workload sharing and offloading. Read replicas can be in another region (uses asynchronous replication) RDS with Multi-AZ is within a region only DynamoDB with Global Tables and Cross Region Replication is a multi-master database configuration. The solution does not ask for multi-region resilience or a multi-master database. The requirement is simply to serve read traffic from the other regions EC2 instances with EBS replication is not a suitable solution. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- DynamoDB with Global Tables
- EC2 instances with EBS replication
- RDS with Multi-AZ

Q37)

You work as an Enterprise Architect for a global organization which employs 20,000 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 enable users to authenticate using their existing identities and access AWS resources (including the AWS Management Console) using single sign-on (SSO).

What is the simplest way to enable SSO to the AWS management console using the existing domain?

- Launch a large AWS Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication
- Install a Microsoft Active Directory Domain Controller on AWS and add it into your existing on-premise domain
- ✅ Launch an Enterprise Edition AWS Active Directory Service for Microsoft Active Directory and setup trust relationships with your on-premise domain

Explanation:-With the AWS Active Directory Service for Microsoft Active Directory you can setup trust relationships to extend authentication from on-premises Active Directories into the AWS cloud. You can also use Active Directory credentials to authenticate to the AWS management console without having to set up SAML authentication. It is a fully managed AWS service on AWS infrastructure and is the best choice if you have more than 5000 users and/or need a trust relationship set up. You could install a Microsoft AD DC on an EC2 instance and add it to the existing domain.

However, you would then have to setup federation / SAML infrastructure for SSO. This is not therefore the simplest solution AWS Simple AD does not support trust relationships or synchronisation with Active Directory AD Connector would be a good solution for this use case however only supports up to 5,000 users. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

- Use a large AWS Simple AD in AWS

Q38) You are creating a CloudFormation Stack that will create EC2 instances that will record log files to an S3 bucket. When creating the template which optional section is used to return the name of the S3 bucket?

- Resources
- ✅ Outputs

Explanation:-The optional Outputs section declares output values that you can import into other stacks (to create cross-stack references), return in response (to describe stack calls), or view on the AWS CloudFormation console. For example, you can output the S3 bucket name for a stack to make the bucket easier to find Template elements include: File format and version (mandatory) List of resources and associated configuration values (mandatory) Template parameters (optional) Output values (optional) List of data tables (optional). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/ https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/outputs-section-structure.html

- Mappings
- Parameters

Q39) You need to upload a large (2GB) file to an S3 bucket. What is the recommended way to upload a single large file to an S3 bucket?

- Use a single PUT request to upload the large file
- ✅ Use Multipart Upload

Explanation:-In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation. The largest object that can be uploaded in a single PUT is 5 gigabytes Snowball is used for migrating large quantities (TB/PB) of data into AWS, it is overkill for this requirement AWS Import/Export is a service in which you send in HDDs with data on to AWS and they import your data into S3. It is not used for single files. References: https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Use AWS Import/Export
- Use Amazon Snowball

Q40)

You need to run a production process that will use several EC2 instances and run constantly on an ongoing basis. The process cannot be interrupted or restarted without issue.

Which EC2 pricing model would be best for this workload?

- Spot instances
- ✅ Reserved instances

Explanation:-In this scenario for a stable process that will run constantly on an ongoing basis RIs will be the most affordable solution RIs provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. You have the flexibility to change families, OS types, and tenancies while benefitting from RI pricing when you use Convertible RIs Spot is more suited to short term jobs that can afford to be interrupted and offer the lowest price of all options On-demand is useful for short term ad-hoc requirements for which the job cannot afford to be interrupted and are typically more expensive than Spot instances There's no such thing as flexible instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://aws.amazon.com/ec2/pricing/reserved-instances/

- On-demand instances
- Flexible instances

Q41)

Some data has become corrupt in an RDS database you manage. You are planning to use point-in-time restore to recover the data to the last known good configuration.

Which of the following statements is correct about restoring an RDS database to a specific point-in-time? (choose 2)

- You can restore up to the last 1 minute
- ✅ You can restore up to the last 5 minutes

Explanation:-Restored DBs will always be a new RDS instance with a new DNS endpoint and you can restore up to the last 5 minutes You cannot restore from a DB snapshot to an existing DB – a new instance is created when you restore Only default DB parameters and security groups are restored – you must manually associate all other DB parameters and SGs. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/ https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIT.html

- The database restore overwrites the existing database
- ✅ The default DB security group is applied to the new DB instance

Explanation:-Restored DBs will always be a new RDS instance with a new DNS endpoint and you can restore up to the last 5 minutes You cannot restore from a DB snapshot to an existing DB – a new instance is created when you restore Only default DB parameters and security groups are restored – you must manually associate all other DB parameters and SGs. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/ https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIT.html

---

Q42)

You are using a series of Spot instances that process messages from an SQS queue and store results in a DynamoDB table. Shortly after picking up a message from the queue AWS terminated the Spot instance. The Spot instance had not finished processing the message.

What will happen to the message?

- The results may be duplicated in DynamoDB as the message will likely be processed multiple times
- The message will remain in the queue and be immediately picked up by another instance
- The message will be lost as it would have been deleted from the queue when processed
- ✅ The message will become available for processing again after the visibility timeout expires

Explanation:-The visibility timeout is the amount of time a message is invisible in the queue after a reader picks up the message. If a job is processed within the visibility timeout the message will be deleted. If a job is not processed within the visibility timeout the message will become visible again (could be delivered twice). The maximum visibility timeout for an Amazon SQS message is 12 hours The message will not be lost and will not be immediately picked up by another instance. As mentioned above it will be available for processing in the queue again after the timeout expires As the instance had not finished processing the message it should only be fully processed once. Depending on your application process however it is possible some data was written to DynamoDB. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/

Q43)

You are trying to SSH into an EC2 instance running Linux but cannot connect. The EC2 instance has been launched in a public subnet with an Internet Gateway. Upon investigation you have verified that the instance has a public IP address and that the route table does reference the Internet Gateway correctly.

What else needs to be checked to enable connectivity?

- Check that there is a Bastion Host in the subnet and connect to it first
- Check that the VPN is configured correctly
- ✅ Check that the Security Groups and Network ACLs have the correct rules configured

Explanation:-Security Groups and Network ACLs do need to be configured to enable connectivity. Check the there relevant rules exist to allow port 22 inbound to your EC2 instance Bastion Hosts are used as an admin tools so you can connect to a single, secured EC2 instance and then jump from there to other instances (typically in private subnets but not always) The subnet CIDR block is configured automatically as part of the creation of the VPC/subnet so should not be the issue here You do not need a VPN connection to connect to an instance in a public subnet. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Check that the subnet CIDR block is referenced properly in the route table

---

Q44)

Your company runs a two-tier application on the AWS cloud that is composed of a web front-end and an RDS database. The web front-end uses multiple EC2 instances in multiple Availability Zones (AZ) in an Auto Scaling group behind an Elastic Load Balancer. Your manager is concerned about a single point of failure in the RDS database layer.

What would be the most effective approach to minimizing the risk of an AZ failure causing an outage to your database layer?

- Take a snapshot of the database
- Create a Read Replica of the RDS DB instance in another AZ
- ✅ Enable Multi-AZ for the RDS DB instance

Explanation:-Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it. This provides a DR solution as if the AZ in which the primary DB resides fails, multi-AZ will automatically fail over to the replica instance with minimal downtime Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas do not provide HA/DR as you cannot fail over to a read replica. They are used purely for offloading read requests from the primary DB Taking a snapshot of the database is useful for being able to recover from a failure so you can restore the database. However, this does not prevent an outage from happening as there will be significant downtime while you try and restore the snapshot to a new DB instance in another AZ Increasing the DB instance size will not provide any benefits to enabling high availability or fault tolerance, it will only serve to improve the performance of the DB. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- Increase the DB instance size

Q45)

You would like to create a highly available web application that serves static content using multiple On-Demand EC2 instances.

Which of the following AWS services will help you to achieve this? (choose 2)

- ✅ Multiple Availability Zones

Explanation:-None of the answer options present the full solution. However, you have been asked which services will help you to achieve the desired outcome. In this case we need high availability for on-demand EC2 instances. A single Auto Scaling Group will enable the on-demand instances to be launched into multiple availability zones with an elastic load balancer distributing incoming connections to the available EC2 instances. This provides high availability and elasticity Amazon S3 and CloudFront could be used to serve static content from an S3 bucket, however the question states that the web application runs on EC2 instances DynamoDB and ElastiCache are both database services, not web application services, and cannot help deliver high availability for EC2 instances Direct Connect is used for connecting on-premise data centers into AWS using a private network connection and does not help in this situation at all. 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/elastic-load-balancing/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- ✅ Elastic Load Balancer and Auto Scaling

Explanation:-None of the answer options present the full solution. However, you have been asked which services will help you to achieve the desired outcome. In this case we need high availability for on-demand EC2 instances. A single Auto Scaling Group will enable the on-demand instances to be launched into multiple availability zones with an elastic load balancer distributing incoming connections to the available EC2 instances. This provides high availability and elasticity Amazon S3 and CloudFront could be used to serve static content from an S3 bucket, however the question states that the web application runs on EC2 instances DynamoDB and ElastiCache are both database services, not web application services, and cannot help deliver high availability for EC2 instances Direct Connect is used for connecting on-premise data centers into AWS using a private network connection and does not help in this situation at all. 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/elastic-load-balancing/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- DynamoDB and ElastiCache
- Direct Connect

Q46)

You are a Solutions Architect at Digital Cloud Training. A client of yours is using API Gateway for accepting and processing a large number of API calls to AWS Lambda. The client痴 business is rapidly growing and he is therefore expecting a large increase in traffic to his API Gateway and AWS Lambda services.The client has asked for advice on ensuring the services can scale without any reduction in performance.

What advice would you give to the client? (choose 2)

- ✅ API Gateway scales up to the default throttling limit, with some additional burst capacity available

Explanation:-API Gateway can scale to any level of traffic received by an API. API Gateway scales up to the default throttling limit of 10,000 requests per second, and can burst past that up to 5,000 RPS. Throttling is used to protect back-end instances from traffic spikes Lambda uses continuous scaling scales out not up. Lambda scales concurrently executing functions up to your default limit (1000) API Gateway does not use provisioned throughput - this is something that is used to provision performance in DynamoDB API Gateway can scale past the default throttling limits (they are not fixed, you just have to apply to have them adjusted) 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/

- API Gateway scales manually through the assignment of provisioned throughput
- ✅ AWS Lambda scales concurrently executing functions up to your default limit

Explanation:-API Gateway can scale to any level of traffic received by an API. API Gateway scales up to the default throttling limit of 10,000 requests per second, and can burst past that up to 5,000 RPS. Throttling is used to protect back-end instances from traffic spikes Lambda uses continuous scaling scales out not up. Lambda scales concurrently executing functions up to your default limit (1000) API Gateway does not use provisioned throughput - this is something that is used to provision performance in DynamoDB API Gateway can scale past the default throttling limits (they are not fixed, you just have to apply to have them adjusted) 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/

- API Gateway can only scale up to the fixed throttling limits

---

Q47)

An application you manage uses Auto Scaling and a fleet of EC2 instances. You recently noticed that Auto Scaling is scaling the number of instances up and down multiple times in the same hour. You need to implement a remediation to reduce the amount of scaling events. The remediation must be cost-effective and preserve elasticity

What design changes would you implement? (choose 2)

- ✅ Modify the CloudWatch alarm period that triggers your Auto Scaling scale down policy

Explanation:-The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect so this would help. After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities The CloudWatch Alarm Evaluation Period is the number of the most recent data points to evaluate when determining alarm state. This would help as you can increase the number of datapoints required to trigger an alarm The order in which Auto Scaling terminates instances is not the issue here, the problem is that the workload is dynamic and Auto Scaling is constantly reacting to change and launching or terminating instances References: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html#alarm-evaluation https://digitalcloud.guru/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- ✅ Modify the Auto Scaling group cool-down timers

Explanation:-The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect so this would help. After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities The CloudWatch Alarm Evaluation Period is the number of the most recent data points to evaluate when determining alarm state. This would help as you can increase the number of datapoints required to trigger an alarm The order in which Auto Scaling terminates instances is not the issue here, the problem is that the workload is dynamic and Auto Scaling is constantly reacting to change and launching or terminating instances References: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html#alarm-evaluation https://digitalcloud.guru/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- Modify the Auto Scaling group termination policy to terminate the oldest instance first
- Modify the Auto Scaling policy to use scheduled scaling actions

---

Q48)

An EBS-backed EC2 instance has been configured with some proprietary software that uses an embedded license. You need to move the EC2 instance to another Availability Zone (AZ) within the region.

How can this be accomplished? Choose the best answer.

- Use the AWS Management Console to select a different AZ for the existing instance
- ✅ Create an image from the instance. Launch an instance from the AMI in the destination AZ

Explanation:-The easiest and recommended option is to create an AMI (image) from the instance and launch an instance from the AMI in the other AZ. AMIs are backed by snapshots which in turn are backed by S3 so the data is available from any AZ within the region You can take a snapshot, launch an instance in the destination AZ. Stop the instance, detach its root volume, create a volume from the snapshot you took and attach it to the instance. However, this is not the best option There痴 no way to move an EC2 instance from the management console You cannot perform a copy operation to move the instance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://aws.amazon.com/premiumsupport/knowledge-center/move-ec2-instance/

- Take a snapshot of the instance. Create a new EC2 instance and perform a restore from the snapshot
- Perform a copy operation to move the EC2 instance to the destination AZ

Q49)

Your manager has asked you to explain how Amazon ElastiCache may assist with the company痴 plans to improve the performance of database queries.

Which of the below statements is a valid description of the benefits of Amazon ElastiCache? (Choose 2)

✅ ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud

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 ElastiCache is best for scenarios where the DB load is based on Online Analytics Processing (OLAP) transactions not Online Transaction Processing (OLTP) Elasticache EC2 nodes cannot be accessed from the Internet, nor can they be accessed by EC2 instances in other VPCs You cannot mix Memcached and Redis in a cluster References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

⚫ ElastiCache can form clusters using a mixture of Memcached and Redis caching engines, allowing you to take advantage of the best features of each caching engine

⚫ ElastiCache is best suited for scenarios where the data base load type is OLTP

✅ 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

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 ElastiCache is best for scenarios where the DB load is based on Online Analytics Processing (OLAP) transactions not Online Transaction Processing (OLTP) Elasticache EC2 nodes cannot be accessed from the Internet, nor can they be accessed by EC2 instances in other VPCs You cannot mix Memcached and Redis in a cluster References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

Q50)

You have been tasked with building an ECS cluster using the EC2 launch type and need to ensure container instances can connect to the cluster. A colleague informed you that you must ensure the ECS container agent is installed on your EC2 instances. You have selected to use the Amazon ECS-optimized AMI.

Which of the statements below are correct? (Choose 2)

✅ You can install the ECS container agent on any Amazon EC2 instance that supports the Amazon ECS specification

Explanation:-The ECS container agent allows container instances to connect to the cluster nd runs on each infrastructure resource on an ECS cluster. 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). It is available for Linux and Windows The ECS container agent does not need to be installed for all AMIs as it is included in the Amazon ECS optimized AMI With the EC2 launch type the container agent is not installed on AWS managed infrastructure - however this is true for the Fargate launch type You can install the EC2 container agent on Windows instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

⚫ The Amazon ECS container agent is installed on the AWS managed infrastructure used for tasks using the EC2 launch type so you don't need to do anything

⚫ The Amazon ECS container agent must be installed for all AMIs

✅ The Amazon ECS container agent is included in the Amazon ECS-optimized AMI

Explanation:-The ECS container agent allows container instances to connect to the cluster nd runs on each infrastructure resource on an ECS cluster. 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). It is available for Linux and Windows The ECS container agent does not need to be installed for all AMIs as it is included in the Amazon ECS optimized AMI With the EC2 launch type the container agent is not installed on AWS managed infrastructure - however this is true for the Fargate launch type You can install the EC2 container agent on Windows instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/
