Answer Sheet

Q1) You would like to share some documents with public users accessing an S3 bucket over the Internet. What are two valid methods of granting public read permissions so you can share the documents? (choose 2)

✓ Use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket granting read access to public anonymous users
Explanation:-Access policies define access to resources and can be associated with resources (buckets and objects) and users You can use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket. Bucket policies can be used to grant permissions to objects You can define permissions on objects when uploading and at any time afterwards using the AWS Management Console. You cannot use a bucket ACL to grant permissions to objects within the bucket. You must explicitly assign the permissions to each object through an ACL attached as a subresource to that object Using an EC2 instance as a bastion host to share the documents is not a feasible or scalable solution You can configure an S3 bucket as a static website and use CloudFront as a front-end however this is not necessary just to share the documents and imposes some constraints on the solution. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/
● Share the documents using CloudFront and a static website
✓ Grant public read access to the objects when uploading
Explanation:-Access policies define access to resources and can be associated with resources (buckets and objects) and users You can use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket. Bucket policies can be used to grant permissions to objects You can define permissions on objects when uploading and at any time afterwards using the AWS Management Console. You cannot use a bucket ACL to grant permissions to objects within the bucket. You must explicitly assign the permissions to each object through an ACL attached as a subresource to that object Using an EC2 instance as a bastion host to share the documents is not a feasible or scalable solution You can configure an S3 bucket as a static website and use CloudFront as a front-end however this is not necessary just to share the documents and imposes some constraints on the solution. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/
● Grant public read on all objects using the S3 bucket ACL

Q2)

A Solutions Architect is designing an authentication solution using the AWS STS that will provide temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users).

What supported sources are available to the Architect for users? (choose 2)

✓ Another AWS account
Explanation:-The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users) Federation can come from three sources: - Federation (typically AD) - Federation with Mobile Apps (e.g. Facebook, Amazon, Google or other Open ID providers) - Cross account access (another AWS account) The question has asked for supported sources for users. Cognito user pools contain users, but identity pools do not You cannot use STS with local users on a PC or an EC2 instance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/
● EC2 instance
✓ OpenID Connect
Explanation:-The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users) Federation can come from three sources: - Federation (typically AD) - Federation with Mobile Apps (e.g. Facebook, Amazon, Google or other Open ID providers) - Cross account access (another AWS account) The question has asked for supported sources for users. Cognito user pools contain users, but identity pools do not You cannot use STS with local users on a PC or an EC2 instance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/
● A local user on a user's PC

Q3)

You are building an application that will collect information about user behavior. The application will rapidly ingest large amounts of dynamic data and requires very low latency. The database must be scalable without incurring downtime.

Which database would you recommend for this scenario?

● RedShift
✓ DynamoDB
Explanation:-Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability Push button scaling means that you can scale the DB at any time without incurring downtime DynamoDB provides low read and write latency RDS uses EC2 instances so you have to change your instance type/size in order to scale compute vertically RedShift uses EC2 instances as well so you need to choose your instance type/size for scaling compute vertically, but you can also scale horizontally by adding more nodes to the cluster Rapid ingestion of dynamic data is not an ideal use case for RDS or RedShift References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/
● RDS with MySQL
● RDS with Microsoft SQL

Q4) A Solutions Architect is building a complex application with several back-end APIs. The architect is considering using Amazon API Gateway. With Amazon API Gateway what are features that assist with creating and managing APIs? (Choose 2)

✓ You can operate multiple API versions and multiple stages for each version simultaneously
Explanation:-Metering – define plans that meter and restrict third-party developer access to APIs Lifecycle Management – Operate multiple API versions and multiple stages for each version simultaneously so that existing applications can continue to call previous versions after new API versions are published References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/
● You can define the maintenance window or AWS will schedule a 30 minute window
● Flexible message delivery over multiple transport protocols
✓ You can define plans that meter and restrict third-party developer access to APIs
Explanation:-Metering – define plans that meter and restrict third-party developer access to APIs Lifecycle Management – Operate multiple API versions and multiple stages for each version simultaneously so that existing applications can continue to call previous versions after new API versions are published References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-

delivery/amazon-api-gateway/

Q5)

Your company would like to restrict the ability of most users to change their own passwords whilst continuing to allow a select group of users within specific user groups.

What is the best way to achieve this? (choose 2)

● Disable the ability for all users to change their own passwords using the AWS Security Token Service
● Create an IAM Role that grants users the ability to change their own password and attach it to the groups that contain the users
✓ Create an IAM Policy that grants users the ability to change their own password and attach it to the groups that contain the users
Explanation:-A password policy can be defined for enforcing password length, complexity etc. (applies to all users) You can allow or disallow the ability to change passwords using an IAM policy and you should attach this to the group that contains the users, not to the individual users themselves You cannot use an IAM role to perform this function The AWS STS is not used for controlling password policies References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/
✓ Under the IAM Password Policy deselect the option to allow users to change their own passwords
Explanation:-A password policy can be defined for enforcing password length, complexity etc. (applies to all users) You can allow or disallow the ability to change passwords using an IAM policy and you should attach this to the group that contains the users, not to the individual users themselves You cannot use an IAM role to perform this function The AWS STS is not used for controlling password policies. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

Q6)

A colleague from your company's IT Security team has notified you of an Internet-based threat that affects a certain port and protocol combination. You have conducted an audit of your VPC and found that this port and protocol combination is allowed on an Inbound Rule with a source of 0.0.0.0/0. You have verified that this rule only exists for maintenance purposes and need to make an urgent change to block the access.

What is the fastest way to block access from the Internet to the specific ports and protocols?

● Add a deny rule to the security group with a higher priority
● Delete the security group
✓ Update the security group by removing the rule
Explanation:-Security group membership can be changed whilst instances are running Any changes to security groups will take effect immediately You can only assign permit rules in a security group, you cannot assign deny rules If you delete the security you will remove all rules and potentially cause other problems You do need to make the update, as it's the VPC based resources you're concerned about. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/
● You don't need to do anything; this rule will only allow access to VPC based resources

Q7)

You are a Solutions Architect at Digital Cloud Training. One of your clients has requested that you design a solution for distributing load across a number of EC2 instances across multiple AZs within a region. Customers will connect to several different applications running on the client's servers through their browser using multiple domain names and SSL certificates. The certificates are stored in AWS Certificate Manager (ACM).

What is the optimal architecture to ensure high availability, cost effectiveness, and performance?

● Launch a single ALB, configure host-based routing for the domain names and bind an SSL certificate to each routing rule
● Launch multiple ALBs and bind separate SSL certificates to each ELB
✓ Launch a single ALB and bind multiple SSL certificates to the same secure listener. Clients will use the Server Name Indication (SNI) extension
Explanation:-You can use a single ALB and bind multiple SSL certificates to the same listener With Server Name Indication (SNI) a client indicates the hostname to connect to. SNI supports multiple secure websites using a single secure listener You cannot have the same port in multiple listeners so adding multiple listeners would not work. Also, when using standard HTTP/HTTPS the port will always be 80/443 so you must be able to receive traffic on the same ports for multiple applications and still be able to forward to the correct instances. This is where host-based routing comes in With host-based routing you can route client requests based on the Host field (domain name) of the HTTP header allowing you to route to multiple domains from the same load balancer (and share the same listener) You do not need multiple ALBs and it would not be cost-effective. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/
● Launch a single ALB and bind multiple SSL certificates to multiple secure listeners

Q8)

A Linux instance running in your VPC requires some configuration changes to be implemented locally and you need to run some commands.

Which of the following can be used to securely connect to the instance?

● Public key
✓ Key pairs
Explanation:-A key pair consists of a public key that AWS stores, and a private key file that you store For Windows AMIs, the private key file is required to obtain the password used to log into your instance For Linux AMIs, the private key file allows you to securely SSH into your instance The "EC2 password" might refer to the operating system password. By default you cannot login this way to Linux and must use a key pair. However, this can be enabled by setting a password and updating the /etc/ssh/sshd_config file You cannot login to an EC2 instance using certificates/public keys, References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/
● EC2 password
● SSL/TLS certificate

Q9)

One of your EC2 instances runs an application process that saves user data to an attached EBS volume. The EBS volume was

attached to the EC2 instance after it was launched and is unencrypted. You would like to encrypt the data that is stored on the volume as it is considered sensitive however you cannot shutdown the instance due to other application processes that are running.

What is the best method of applying encryption to the sensitive data without any downtime?

● Unmount the volume and enable server-side encryption. Re-mount the EBS volume

✓ Create and mount a new encrypted EBS volume. Move the data to the new volume and then delete the old volume

Explanation:-You cannot restore a snapshot of a root volume without downtime There is no direct way to change the encryption state of a volume Either create an encrypted volume and copy data to it or take a snapshot, encrypt it, and create a new encrypted volume from the snapshot. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

● Create an encrypted snapshot of the current EBS volume. Restore the snapshot to the EBS volume

● Leverage the AWS Encryption CLI to encrypt the data on the volume

---

Q10)

You are a Solutions Architect at Digital Cloud Training. A client has requested a design for a highly-available, fault tolerant architecture for the web and app tiers of a three-tier application. The requirements are as follows:

- Web instances will be in a public subnet and app instances will be in a private subnet

- Connections to EC2 instances should be automatically distributed across AZs

- A minimum of 12 web server EC2 instances must be running at all times

- A minimum of 6 app server EC2 instances must be running at all times

- The failure of a single availability zone (AZ) must not affect The availability of The application or result in a reduction of capacity beneath The stated requirements

Which of the following design options would be the most suitable and cost-effective solution?

● One Auto Scaling Group with a minimum of 12 EC2 instances for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 6 EC2 instances for the app layer. A single Internet-facing ALB using 3 AZs and two target groups for the web and app layers

● One Auto Scaling Group with a minimum of 18 EC2 instances for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 9 EC2 instances for the app layer. A single Internet-facing ALB using 3 AZs and two target groups for the web and app layers

● One Auto Scaling Group using 3 AZs and a minimum of 12 EC2 instances behind an Internet facing ALB for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 6 EC2 instances behind an internal-only ALB for the app layer

✓ One Auto Scaling Group using 3 AZs and a minimum of 18 EC2 instances behind an Internet facing ALB for the web layer. One Auto Scaling Group using 3 AZs and a minimum of 9 EC2 instances behind an internal-only ALB for the app layer

Explanation:-Simple scaling maintains a current number of instances, you can manually change the ASGs min/desired/max and attach/detach instances. Auto Scaling will try to distribute EC2 instances evenly across AZs In this scenario you must have a minimum of 12 instances running in the event of an AZ failure, therefore with 18 instances across 3 AZs if one AZ fails you still have enough instances ELBs can be Internet-facing or internal-only. Remember that internet-facing ELBs have public IPs, whereas internal-only ELBs have private IPs have public IPs. Therefore, you must have 2 ELBs, one for the web layer and one for the app layer. Otherwise the web layer would have to hairpin the traffic back to the public IP of the ELB rather than forwarding it to the internal ELB and this is not a supported configuration. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q11)

A customer has asked you to recommend the best solution for a highly available database. The database is a relational OLTP type of database and the customer does not want to manage the operating system the database runs on. Failover between AZs must be automatic.

Which of the below options would you suggest to the customer?

● Install a relational database on EC2 instances in multiple AZs and create a cluster

✓ Use RDS in a Multi-AZ configuration

Explanation:-Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. With RDS you can configure Multi-AZ which creates a replica in another AZ and synchronously replicates to it (DR only) RedShift is used for analytics OLAP not OLTP If you install a DB on an EC2 instance you will need to manage to OS yourself and the customer wants it to be managed for them DynamoDB is a managed database of the NoSQL type. NoSQL DBs are not relational DBs. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

● Use DynamoDB

● Use RedShift in a Multi-AZ configuration

Q12) You are troubleshooting a connectivity issue where you cannot connect to an EC2 instance in a public subnet in your VPC from the Internet. Which of the configuration items in the list below would you check first? (choose 2)

✓ The security group attached to the EC2 instance has an inbound rule allowing the traffic

Explanation:-Public subnets are subnets that have: “Auto-assign public IPv4 address?? set to “Yes?? which will assign a public IP The subnet route table has an attached Internet Gateway The instance will also need to a security group with an inbound rule allowing the traffic EC2 instances always have a private IP address assigned. When using a public subnet with an Internet Gateway the instance needs a public IP to be addressable from the Internet NAT gateways are used to enable outbound Internet access for instances in private subnets. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

● The subnet route table has an attached NAT Gateway

● There is a NAT Gateway installed in the subnet

✓ The subnet has “Auto-assign public IPv4 address" set to “Yes"

Explanation:-Public subnets are subnets that have: “Auto-assign public IPv4 address?? set to “Yes?? which will assign a public IP The subnet route table has an attached Internet Gateway The instance will also need to a security group with an inbound rule allowing the traffic EC2 instances always have a private IP address assigned. When using a public subnet with an Internet Gateway the instance needs a public IP to be addressable from the Internet NAT gateways are used to enable outbound Internet access for instances in private subnets. References:

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

Q13)

You would like to provide some on-demand and live streaming video to your customers. The plan is to provide the users with both the media player and the media files from the AWS cloud. One of the features you need is for the content of the media files to begin playing while the file is still being downloaded.

What AWS services can deliver these requirements? (choose 2)

● Store the media files on an EC2 instance

✓ Store the media files in an S3 bucket

Explanation:-For serving both the media player and media files you need two types of distributions: - A web distribution for the media player - An RTMP distribution for the media files RTMP: - Distribute streaming media files using Adobe Flash Media Server's RTMP protocol - Allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location - Files must be stored in an S3 bucket (not an EBS volume or EC2 instance). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

● Use CloudFront with an RTMP distribution

✓ Use CloudFront with a Web and RTMP distribution

Explanation:-For serving both the media player and media files you need two types of distributions: - A web distribution for the media player - An RTMP distribution for the media files RTMP: - Distribute streaming media files using Adobe Flash Media Server's RTMP protocol - Allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location - Files must be stored in an S3 bucket (not an EBS volume or EC2 instance). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

Q14)

There is a new requirement to implement in-memory caching for a Financial Services application due to increasing read-heavy load. The data must be stored persistently. Automatic failover across AZs is also required.

Which two items from the list below are required to deliver these requirements? (choose 2)

✓ Multi-AZ with Cluster mode and Automatic Failover enabled

Explanation:-Redis engine stores data persistently Memached engine does not store data persistently Redis engine supports Multi-AZ using read replicas in another AZ in the same region You can have a fully automated, fault tolerant ElastiCache-Redis implementation by enabling both cluster mode and multi-AZ failover Memcached engine does not support Multi-AZ failover or replication. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/

● ElastiCache with the Memcached engine

✓ ElastiCache with the Redis engine

Explanation:-Redis engine stores data persistently Memached engine does not store data persistently Redis engine supports Multi-AZ using read replicas in another AZ in the same region You can have a fully automated, fault tolerant ElastiCache-Redis implementation by enabling both cluster mode and multi-AZ failover Memcached engine does not support Multi-AZ failover or replication. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/

● Multiple nodes placed in different AZs

Q15) A Solutions Architect is designing a data archive strategy using Amazon Glacier. The Architect needs to explain the features of the service to his manager, which statements about Glacier are correct? (choose 2)

✓ Uploading archives is synchronous; downloading archives is asynchronous

Explanation:-Glacier objects are visible through S3 only (not Glacier directly) The contents of an archive that has been uploaded cannot be modified Uploading archives is synchronous Downloading archives is asynchronous Retrieval can take a few hours. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

● The contents of an archive can be modified after uploading

✓ Glacier objects are visible through S3 only

Explanation:-Glacier objects are visible through S3 only (not Glacier directly) The contents of an archive that has been uploaded cannot be modified Uploading archives is synchronous Downloading archives is asynchronous Retrieval can take a few hours. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

● Retrieval is immediate

Q16)

The association between a poll-based source and a Lambda function is called the event source mapping. Event sources maintain the mapping configuration except for stream-based services such as ________ and ________ for which the configuration is made on the Lambda side and Lambda performs the polling.

Fill in the blanks from the options below (choose 2)

● IoT Button

✓ Kinesis

Explanation:-Event sources are mapped to Lambda functions Event sources maintain the mapping configuration except for stream-based services (e.g. DynamoDB, Kinesis) for which the configuration is made on the Lambda side and Lambda performs the polling This question is really just asking you to identify which of the listed services are stream-based services. DynamoDB and Kinesis are both used for streaming data. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

● S3

✓ DynamoDB

Explanation:-Event sources are mapped to Lambda functions Event sources maintain the mapping configuration except for stream-based services (e.g. DynamoDB, Kinesis) for which the configuration is made on the Lambda side and Lambda performs the polling This question is really just asking you to identify which of the listed services are stream-based services. DynamoDB and Kinesis are both used for streaming data. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

Q17)

The data scientists in your company are looking for a service that can process and analyze real-time, streaming data. They would like to use standard SQL queries to query the streaming data.

Which combination of AWS services would deliver these requirements?

● ElastiCache and EMR
✓ Kinesis Data Streams and Kinesis Data Analytics
Explanation:-Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs Amazon Kinesis Data Analytics is the easiest way to process and analyze real-time, streaming data. Kinesis Data Analytics can use standard SQL queries to process Kinesis data streams and can ingest data from Kinesis Streams and Kinesis Firehose but Firehose cannot be used for running SQL queries DynamoDB is a NoSQL database that can be used for storing data from a stream but cannot be used to process or analyze the data or to query it with SQL queries. Elastic Map Reduce (EMR) is a hosted Hadoop framework and is not used for analytics on streaming data. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/
● DynamoDB and EMR
● Kinesis Data Streams and Kinesis Firehose

Q18) You are a Solutions Architect at a media company and you need to build an application stack that can receive customer comments from sporting events. The application is expected to receive significant load that could scale to millions of messages within a short space of time following high-profile matches. As you are unsure of the load required for the database layer what is the most cost-effective way to ensure that the messages are not dropped?

● Use DynamoDB and provision enough write capacity to handle the highest expected load
● Write the data to an S3 bucket, configure RDS to poll the bucket for new messages
✓ Create an SQS queue and modify the application to write to the SQS queue. Launch another application instance the polls the queue and writes messages to the database
Explanation:-Amazon Simple Queue Service (Amazon SQS) is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers and is used for distributed/decoupled applications This is a great use case for SQS as the messages you don't have to over-provision the database layer or worry about messages being dropped RDS Auto Scaling does not exist. With RDS you have to select the underlying EC2 instance type to use and pay for that regardless of the actual load on the DB With DynamoDB there are now 2 pricing options: - Provisioned capacity has been around forever and is one of the incorrect answers to this question. With provisioned capacity you have to specify the number of read/write capacity units to provision and pay for these regardless of the load on the database. - With the the new On-demand capacity mode DynamoDB is charged based on the data reads and writes your application performs on your tables. You do not need to specify how much read and write throughput you expect your application to perform because DynamoDB instantly accommodates your workloads as they ramp up or down. it might be a good solution to this question but is not an available option. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/
● Use RDS Auto Scaling for the database layer which will automatically scale as required

---

Q19)

You are a Solutions Architect at Digital Cloud Training. A large multi-national client has requested a design for a multi-region, multi-master database. The client has requested that the database be designed for fast, massively scaled applications for a global user base. The database should be a fully managed service including the replication.

Which AWS service can deliver these requirements?

✓ DynamoDB with Global Tables and Cross Region Replication
Explanation:-Cross-region replication allows you to replicate across regions: - Amazon DynamoDB global tables provides a fully managed solution for deploying a multi-region, multi-master database - When you create a global table, you specify the AWS regions where you want the table to be available - DynamoDB performs all of the necessary tasks to create identical tables in these regions, and propagate ongoing data changes to all of them RDS with Multi-AZ is not multi-master (only one DB can be written to at a time), and does not span regions S3 is an object store not a multi-master database There is no such thing as EBS replication. You could build your own database stack on EC2 with DB-level replication but that is not what is presented in the answer. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/
● S3 with Cross Region Replication
● RDS with Multi-AZ
● EC2 instances with EBS replication

Q20)

The application development team in your company has a new requirement for the deployment of a container solution. You plan to use the AWS Elastic Container Service (ECS). The solution should include load balancing of incoming requests across the ECS containers and allow the containers to use dynamic host port mapping so that multiple tasks from the same service can run on the same container host.

Which AWS load balancing configuration will support this?

● You cannot run multiple copies of a task on the same instance, because the ports would conflict
● Use a Network Load Balancer (NLB) and host-based routing
● Use a Classic Load Balancer (CLB) and create a static mapping of the ports
✓ Use an Application Load Balancer (ALB) and map the ECS service to the ALB
Explanation:-It is possible to associate a service on Amazon ECS to an Application Load Balancer (ALB) for the Elastic Load Balancing (ELB) service An Application Load Balancer allows dynamic port mapping. You can have multiple tasks from a single service on the same container instance. The Classic Load Balancer requires that you statically map port numbers on a container instance. You cannot run multiple copies of a task on the same instance, because the ports would conflict An NLB does not support host-based routing (ALB only), and this would not help anyway. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q21) To improve security in your AWS account you have decided to enable multi-factor authentication (MFA). You can authenticate using an MFA device in which two ways? (choose 2)

● Using a key pair

✓ Using the AWS API

Explanation:-You can authenticate using an MFA device in the following ways: Through the AWS Management Console – the user is prompted for a user name, password and authentication code Using the AWS API – restrictions are added to IAM policies and developers can request temporary security credentials and pass MFA parameters in their AWS STS API requests Using the AWS CLI by obtaining temporary security credentials from STS (aws sts get-session-token). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

● Locally to EC2 instances

✓ Through the AWS Management Console

Explanation:-You can authenticate using an MFA device in the following ways: Through the AWS Management Console – the user is prompted for a user name, password and authentication code Using the AWS API – restrictions are added to IAM policies and developers can request temporary security credentials and pass MFA parameters in their AWS STS API requests Using the AWS CLI by obtaining temporary security credentials from STS (aws sts get-session-token). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

Q22)

An application that was recently moved into the AWS cloud has been experiencing some authentication issues. The application is currently configured to authenticate to an on-premise Microsoft Active Directory Domain Controller via a VPN connection. Upon troubleshooting the issues, it seems that latency across the VPN connection is causing authentication to fail. Your company is very cost sensitive at the moment and the administrators of the Microsoft AD do not want to manage any additional directories. You need to resolve the issues quickly.

What is the best solution to solve the authentication issues taking cost considerations into account?

● Use the AWS Active Directory Service for Microsoft Active Directory and create a new domain. Establish a trust relationship with your existing on-premise domain

✓ Install an additional Microsoft Active Directory Domain Controller for your existing domain on EC2 and configure the application to authenticate to the local DC

Explanation:-Direct Connect is an incorrect option as it can take months to provision and a quick resolution has been requested The best answer is to Install an additional Microsoft Active Directory Domain Controller for your existing domain on EC2: - When you build your own you can join an existing on-premise Active Directory domain/directory (replication mode) - You must establish a VPN (on top of Direct Connect if you have it) - Replication mode is less secure than establishing trust relationships AWS Microsoft AD does not support replication mode where replication to an on-premise AD takes place The option to use the AWS Active Directory Service for Microsoft Active Directory and create a new domain is incorrect as it involves creating a new directory which the administrators don't want. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

● Use the AWS Active Directory Service for Microsoft Active Directory and join your existing on-premise domain

● Create an AWS Direct Connect connection to reduce the latency between your company and AWS

Q23)

You are designing an identity, authorization and access management solution for the AWS cloud. The features you need include the ability to manage user accounts and group memberships, create and apply group policies, securely connect to Amazon EC2 instances, and provide Kerberos-based single sign-on (SSO). You do not need to establish trust relationships with other domains, use DNS dynamic update, implement schema extensions or use other advanced directory features.

What would be the most cost-effective solution?

● Use AWS Directory Service for Microsoft AD

✓ Use AWS Simple AD

Explanation:-AWS Simple AD is an inexpensive Active Directory-compatible service with common directory features. It is a standalone, fully managed, directory on the AWS cloud. Simple AD is generally the least expensive option and the best choice for less than 50000 users and don't need advanced AD features. It is powered by SAMBA 4 Active Directory compatible server AD Connector is a directory gateway for redirecting directory requests to an Active Directory service. As you only require simple features and are looking for cost-effectiveness this would not be the best option as you must maintain an Active Directory service The AWS Directory Service for Microsoft AD is a fully managed AWS service on AWS infrastructure.It is the best choice if you have more than 5000 users and/or need a trust relationship set up. In this case you don't need those features and it would be more expensive so isn't the best options Amazon Cloud Directory enables you to build flexible cloud-native directories for organizing hierarchies of data along multiple dimensions, it is not used for authentication use cases. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

● Use Amazon Cloud Directory

● Use AD Connector

Q24)

You work for a company that produces TV commercials. You are planning to run an advertising campaign during a major political event that will be watched by millions of people over several days. It is expected that your website will receive large bursts of traffic following commercial breaks. You have performed an analysis and determined that you will need up to 150 EC2 web instances to process the traffic which is within the client's budgetYou need to ensure you deliver a high quality and consistent user experience whilst not exceeding the client's budget.

How would you design a highly available and elastic solution?

● Create an Auto Scaling Group across multiple AZs with a desired capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG and pre-warm the ALB by contacting AWS prior to the event

● Create an Auto Scaling Group across multiple AZs with a desired capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG

● Create an Auto Scaling Group across multiple AZs with a maximum capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG

✓ Create an Auto Scaling Group across multiple AZs with a maximum capacity of 150 EC2 instances. Launch an Application Load Balancer and specify the same AZs as the ASG and pre-warm the ALB by contacting AWS prior to the event

Explanation:-For this solution you must provide an elastic solution that can scale quickly with demand up to the client's budget limit. Therefore, as the analysis shows you will need up to 150 EC2 instances, which is within the client's budget you should set the ASG with a maximum capacity of 150 EC2 instances so it cannot exceed the budget. If you're anticipating a fast increase in load you can contact AWS and instruct them to pre-warm (provision) additional ELB nodes, this will ensure that the nodes will be ready when needed. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q25) For operational access to your AWS environment you are planning to setup a bastion host implementation. Which of the below are AWS best practices for setting up bastion hosts? (choose 2)

✓ Elastic IP addresses are associated with the bastion instances to make it easier to remember and allow these IP addresses from on-premises firewalls

Explanation:-You can configure EC2 instances as bastion hosts (aka jump boxes) in order to access your VPC instances for management. Bastion hosts are deployed in public (not private) subnets within your VPC. You can use the SSH or RDP protocols to connect to bastion hosts You need to configure a security group with the relevant permissions to allow the SSH or RDP protocols. You can also use security group rules to restrict the IP addresses/CIDRs that can access the bastion host. Bastion hosts can use auto-assigned public IPs or Elastic IPs It is a best practice is to deploy Linux bastion hosts in two AZs, use Auto Scaling (set to 1 to just replace)and Elastic IP addresses Setting the security rule to allow from the 0.0.0.0/0 source would allow any host on the Internet to access your bastion. It's a security best practice to restrict the sources to known (safe) IP addresses or CIDR blocks. You would not want to allow unrestricted access to ports on the bastion host. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

● Bastion hosts are deployed in the private subnets of the VPC

✓ Deploy in 2 AZs and use an Auto Scaling group to ensure that the number of bastion host instances always matches the desired capacity you specify during launch

Explanation:-You can configure EC2 instances as bastion hosts (aka jump boxes) in order to access your VPC instances for management. Bastion hosts are deployed in public (not private) subnets within your VPC. You can use the SSH or RDP protocols to connect to bastion hosts You need to configure a security group with the relevant permissions to allow the SSH or RDP protocols. You can also use security group rules to restrict the IP addresses/CIDRs that can access the bastion host. Bastion hosts can use auto-assigned public IPs or Elastic IPs It is a best practice is to deploy Linux bastion hosts in two AZs, use Auto Scaling (set to 1 to just replace)and Elastic IP addresses Setting the security rule to allow from the 0.0.0.0/0 source would allow any host on the Internet to access your bastion. It's a security best practice to restrict the sources to known (safe) IP addresses or CIDR blocks. You would not want to allow unrestricted access to ports on the bastion host. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

● Access to the bastion hosts is configured to 0.0.0.0/0 for ingress in security groups

Q26)

An application running on an external website is attempting to initiate a request to your company's website on AWS using API calls. A problem has been reported in which the requests are failing with an error that includes the following text:

"Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource"You have been asked to resolve the problem, what is the most likely solution?

● The ACL on the API needs to be updated

✓ Enable CORS on the APIs resources using the selected methods under the API Gateway

Explanation:-Can enable Cross Origin Resource Sharing (CORS) for multiple domain use with Javascript/AJAX: - Can be used to enable requests from domains other the APIs domain - Allows the sharing of resources between different domains - The method (GET, PUT, POST etc) for which you will enable CORS must be available in the API Gateway API before you enable CORS - If CORS is not enabled and an API resource received requests from another domain the request will be blocked - Enable CORS on the APIs resources using the selected methods under the API Gateway IAM policies are not used to control CORS and there is no ACL on the API to update This error would display whether using SSL/TLS or not. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

● The IAM policy does not allow access to the API

● The request is not secured with SSL/TLS

Q27)

You are an entrepreneur building a small company with some resources running on AWS. As you have limited funding you're extremely cost conscious.

Which AWS service can send you alerts via email or SNS topic when you are forecast to exceed your funding capacity so you can take action?

● AWS Billing Dashboard

✓ AWS Budgets

Explanation:-AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. Budget alerts can be sent via email and/or Amazon Simple Notification Service (SNS) topic The AWS Cost Explorer is a free tool that allows you to view charts of your costs The AWS Billing Dashboard can send alerts when you're bill reaches certain thresholds but you must use AWS Budgets to created custom budgets that notify you when you are forecast to exceed a budget The AWS Cost and Usage report tracks your AWS usage and provides estimated charges associated with your AWS account but does not send alerts References: https://aws.amazon.com/aws-cost-management/aws-budgets/

● Cost Explorer

● Cost & Usage reports

Q28) A company is in the process of deploying an Amazon Elastic Map Reduce (EMR) cluster. Which of the statements below accurately describe the EMR service? (choose 2)

● EMR is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud

✓ EMR launches all nodes for a given cluster in the same Amazon EC2 Availability Zone

Explanation:-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. EMR uses Apache Hadoop as its distributed data processing engine which is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), playback, and other processing EMR launches all nodes for a given cluster in the same Amazon EC2 Availability Zone EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/

● EMR makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing

✓ EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3

Explanation:-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. EMR uses Apache Hadoop as its distributed data processing engine which is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), playback, and other processing EMR launches all nodes for a given cluster in the same Amazon EC2 Availability Zone EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/

Q29)

As a SysOps engineer working at Digital Cloud Training, you are constantly trying to improve your processes for collecting log data. Currently you are collecting logs from across your AWS resources using CloudWatch and a combination of standard and custom metrics. You are currently investigating how you can optimize the storage of log files collected by CloudWatch.

Which of the following are valid options for storing CloudWatch log files? (choose 2)

✓ Splunk

Explanation:-Valid options for storing logs include: - CloudWatch Logs - Centralized logging system (e.g. Splunk) - Custom script and store on S3 RedShift, EFS and EBS are not valid options for storing CloudWatch log files. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/

● EFS

✓ CloudWatch Logs

Explanation:-Valid options for storing logs include: - CloudWatch Logs - Centralized logging system (e.g. Splunk) - Custom script and store on S3 RedShift, EFS and EBS are not valid options for storing CloudWatch log files. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/

● EBS

Q30)

Your company uses Amazon Glacier to store files that must be retained for compliance reasons and are rarely accessed. An auditor has requested access to some information that is stored in a Glacier archive. You have initiated an archive retrieval job.

Which factors are important to know about the process from this point? (choose 2)

✓ Amazon Glacier must complete a job before you can get its output

Explanation:-There is a charge if you delete data within 90 days – however we are not talking about deleting data here, just retrieving it Retrieved data is available for 24 hours by default (can be changed) Amazon Glacier must complete a job before you can get its output Glacier automatically encrypts data at rest using AES 256 symmetric keys and supports secure transfer of data over SSL Retrieved data will not be encrypted if it was uploaded unencrypted You do not need an MFA device to access the retrieved files. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

✓ Following retrieval, you have 24 hours to download your data

Explanation:-There is a charge if you delete data within 90 days – however we are not talking about deleting data here, just retrieving it Retrieved data is available for 24 hours by default (can be changed) Amazon Glacier must complete a job before you can get its output Glacier automatically encrypts data at rest using AES 256 symmetric keys and supports secure transfer of data over SSL Retrieved data will not be encrypted if it was uploaded unencrypted You do not need an MFA device to access the retrieved files. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

● There is a charge if you delete data within 90 days

● The retrieved data will always be encrypted

Q31)

A company is considering using EC2 Reserved Instances to reduce cost. The Architect involved is concerned about the potential limitations in flexibility of using RIs instead of On-Demand instances.

Which of the following statements about RIs are useful to the Architect? (choose 2)

● You cannot launch RIs using Auto Scaling Groups

✓ You can use RIs in Placement Groups

Explanation:-Capacity is reserved for a term of 1 or 3 years Standard = commitment of 1 or 3 years, charged whether it's on or off Scheduled = reserved for specific periods of time, accrue charges hourly, billed in monthly increments over the term (1 year) Scheduled RIs match your capacity reservation to a predictable recurring schedule RIs are used for steady state workloads and predictable usage Ideal for applications that need reserved capacity Upfront payments can reduce the hourly rate Can switch AZ within the same region Can change the instance size within the same instance type Instance type modifications are supported for Linux only Cannot change the instance size of Windows RIs Billed whether running or not Can sell reservations on the AWS marketplace Can be used in Auto Scaling Groups Can be used in Placement Groups. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

● There is a fee charged for any RI modifications

✓ RIs can be sold on the Reserved Instance Marketplace

Explanation:-Capacity is reserved for a term of 1 or 3 years Standard = commitment of 1 or 3 years, charged whether it's on or off Scheduled = reserved for specific periods of time, accrue charges hourly, billed in monthly increments over the term (1 year) Scheduled RIs match your capacity reservation to a predictable recurring schedule RIs are used for steady state workloads and predictable usage Ideal for applications that need reserved capacity Upfront payments can reduce the hourly rate Can switch AZ within the same region Can change the instance size within the same instance type Instance type modifications are supported for Linux only Cannot change the instance size of Windows RIs Billed whether running or

not Can sell reservations on the AWS marketplace Can be used in Auto Scaling Groups Can be used in Placement Groups. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

Q32) Your company has recently formed a partnership with another company. Both companies have resources running in the AWS cloud and you would like to be able to access each other's resources using private IP addresses. The resources for each company are in different AWS regions and you need to ensure that fully redundant connectivity is established.You have established a VPC peering connection between the VPCs, what steps need to be taken next to establish connectivity and resource sharing between the VPCs across regions? (choose 2)

✓ Update Security Group rules to allow resource sharing

Explanation:-Peering connections can be created with VPCs in different regions (available in most regions now). Data sent between VPCs in different regions is encrypted (traffic charges apply). You must update route tables to configure routing. You must also update the inbound and outbound rules for VPC security group to reference security groups in the peered VPC When creating a VPC peering connection with another account you need to enter the account ID and VPC ID from the other account You do not use an IPSec VPN or Direct Connect to establish VPC peering, the connections are internal to AWS using the AWS network infrastructure BGP routing configuration is required for Direct Connect but not for VPC peering. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

● Establish an IPSec VPN between the VPCs

● Establish redundant Direct Connect connections between the VPCs

✓ Manually add routes to each VPCs routing tables as required to enable IP connectivity

Explanation:-Peering connections can be created with VPCs in different regions (available in most regions now). Data sent between VPCs in different regions is encrypted (traffic charges apply). You must update route tables to configure routing. You must also update the inbound and outbound rules for VPC security group to reference security groups in the peered VPC When creating a VPC peering connection with another account you need to enter the account ID and VPC ID from the other account You do not use an IPSec VPN or Direct Connect to establish VPC peering, the connections are internal to AWS using the AWS network infrastructure BGP routing configuration is required for Direct Connect but not for VPC peering. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q33)

Several websites you run on AWS use multiple Internet-facing Elastic Load Balancers (ELB) to distribute incoming connections to EC2 instances running web applications. The ELBs are configured to forward using either TCP (layer 4) or HTTP (layer 7) protocols. You would like to start recording the IP addresses of the clients that connect to your web applications.

Which ELB features will you implement with which protocols? (choose 2)

✓ Proxy Protocol and TCP

Explanation:-Proxy protocol for TCP/SSL carries the source (client) IP/port information X-forwarded-for for HTTP/HTTPS carries the source IP/port information In both cases the protocol carries the source IP/port information right through to the web server. If you were happy to just record the source connections on the load balancer you could use access logs References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

✓ X-Forwarded-For request header and HTTP

Explanation:-Proxy protocol for TCP/SSL carries the source (client) IP/port information X-forwarded-for for HTTP/HTTPS carries the source IP/port information In both cases the protocol carries the source IP/port information right through to the web server. If you were happy to just record the source connections on the load balancer you could use access logs. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

● X-Forwarded-For request header and TCP

● Proxy Protocol and HTTP

Q34)

Your company has offices in several locations around the world. Each office utilizes resources deployed in the geographically closest AWS region. You would like to implement connectivity between all of the VPCs so that you can provide full access to each other's resources. As you are security conscious you would like to ensure the traffic is encrypted and does not traverse the public Internet. The topology should be many-to-many to enable all VPCs to access the resources in all other VPCs.

How can you successfully implement this connectivity using only AWS services? (choose 2)

✓ Implement a fully meshed architecture

Explanation:-Peering connections can be created with VPCs in different regions (available in most regions now) Data sent between VPCs in different regions is encrypted (traffic charges apply) You cannot do transitive peering so a hub and spoke architecture would not allow all VPCs to communicate directly with each other. For this you need to establish a mesh topology A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services, it does not provide full VPC to VPC connectivity Using software VPN appliances to connect VPCs together is not the best solution as it is cumbersome, expensive and would introduce bandwidth and latency constraints (amongst other problems). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

✓ Use inter-region VPC peering

Explanation:-Peering connections can be created with VPCs in different regions (available in most regions now) Data sent between VPCs in different regions is encrypted (traffic charges apply) You cannot do transitive peering so a hub and spoke architecture would not allow all VPCs to communicate directly with each other. For this you need to establish a mesh topology A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services, it does not provide full VPC to VPC connectivity Using software VPN appliances to connect VPCs together is not the best solution as it is cumbersome, expensive and would introduce bandwidth and latency constraints (amongst other problems). References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

● Use software VPN appliances running on EC2 instances

● Implement a hub and spoke architecture

Q35)

The company you work for is currently transitioning their infrastructure and applications into the AWS cloud. You are planning

to deploy an Elastic Load Balancer (ELB) that distributes traffic for a web application running on EC2 instances. You still have some application servers running on-premise and you would like to distribute application traffic across both your AWS and on-premises resources.

How can this be achieved?

● This cannot be done, ELBs are an AWS service and can only distributed traffic within the AWS cloud

● Provision an IPSec VPN connection between your on-premises location and AWS and create a CLB that uses cross-zone load balancing to distributed traffic across EC2 instances and on-premises servers

● Provision a Direct Connect connection between your on-premises location and AWS and create a target group on an ALB to use Instance ID based targets for both your EC2 instances and on-premises server

✓ Provision a Direct Connect connection between your on-premises location and AWS and create a target group on an ALB to use IP based targets for both your EC2 instances and on-premises servers

Explanation:-The ALB (and NLB) supports IP addresses as targets Using IP addresses as targets allows load balancing any application hosted in AWS or on-premises using IP addresses of the application back-ends as targets You must have a VPN or Direct Connect connection to enable this configuration to work You cannot use instance ID based targets for on-premises servers and you cannot mix instance ID and IP address target types in a single target group The CLB does not support IP addresses as targets. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/

Q36)

You are undertaking a project to make some audio and video files that your company uses for onboarding new staff members available via a mobile application. You are looking for a cost-effective way to convert the files from their current formats into formats that are compatible with smartphones and tablets. The files are currently stored in an S3 bucket.

What AWS service can help with converting the files?

● Data Pipeline

✓ Elastic Transcoder

Explanation:-Amazon Elastic Transcoder is a highly scalable, easy to use and cost-effective way for developers and businesses to convert (or “transcode??) video and audio files from their source format into versions that will playback on devices like smartphones, tablets and PCs MediaConvert converts file-based content for broadcast and multi-screen delivery Data Pipeline helps you move, integrate, and process data across AWS compute and storage resources, as well as your on-premises resources Rekognition is a deep learning-based visual analysis service. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/media-services/amazon-elastic-transcoder/

● MediaConvert

● Rekognition

Q37)

A company uses CloudFront to provide low-latency access to cached files. An Architect is considering the implications of using CloudFront Regional Edge Caches.

Which statements are correct in relation to this service? (choose 2)

✓ Regional Edge Caches have larger cache-width than any individual edge location, so your objects remain in cache longer at these locations

Explanation:-Regional Edge Caches are located between origin web servers and global edge locations and have a larger cache than any individual edge location, so your objects remain in cache longer at these locations. Regional Edge caches aim to get content closer to users and are enabled by default for CloudFront Distributions (so you don't need to update your distributions) There are no additional charges for using Regional Edge Caches You can write to regional edge caches too. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/ https://aws.amazon.com/about-aws/whats-new/2016/11/announcing-regional-edge-caches-for-amazon-cloudfront/

● There are additional charges for using Regional Edge Caches

✓ Regional Edge Caches are enabled by default for CloudFront Distributions

Explanation:-Regional Edge Caches are located between origin web servers and global edge locations and have a larger cache than any individual edge location, so your objects remain in cache longer at these locations. Regional Edge caches aim to get content closer to users and are enabled by default for CloudFront Distributions (so you don't need to update your distributions) There are no additional charges for using Regional Edge Caches You can write to regional edge caches too. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/ https://aws.amazon.com/about-aws/whats-new/2016/11/announcing-regional-edge-caches-for-amazon-cloudfront/

● Regional Edge Caches are read-only

Q38)

The company you work for has a presence across multiple AWS regions. As part of disaster recovery planning you are formulating a solution to provide a regional DR capability for an application running on a fleet of Amazon EC2 instances that are provisioned by an Auto Scaling Group (ASG). The applications are stateless and read and write data to an S3 bucket. You would like to utilize the current AMI used by the ASG as it has some customizations made to it.

What are the steps you might take to enable a regional DR capability for this application? (choose 2)

✓ Copy the AMI to the DR region and create a new launch configuration for the ASG that uses the AMI

Explanation:-There are two parts to this solution. First you need to copy the S3 data to each region (as the instances are stateless), then you need to be able to deploy instances from an ASG using the same AMI in each regions. - CRR is an Amazon S3 feature that automatically replicates data across AWS Regions. With CRR, every object uploaded to an S3 bucket is automatically replicated to a destination bucket in a different AWS Region that you choose, this enables you to copy the existing data across to each region - AMIs of both Amazon EBS-backed AMIs and instance store-backed AMIs can be copied between regions. You can then use the copied AMI to create a new launch configuration (remember that you cannot modify an ASG launch configuration, you must create a new launch configuration) There's no such thing as Multi-AZ for an S3 bucket (it's an RDS concept) Changing permissions on an AMI doesn't make it usable from another region, the AMI needs to be present within each region to be used. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

● Modify the permissions of the AMI so it can be used across multiple regions

● Enable multi-AZ for the S3 bucket to enable synchronous replication to the DR region

✓ Enable cross region replication on the S3 bucket and specify a destination bucket in the DR region

Explanation:-There are two parts to this solution. First you need to copy the S3 data to each region (as the instances are stateless), then you need to be able to deploy instances from an ASG using the same AMI in each regions. - CRR is an Amazon S3 feature that automatically replicates data across AWS Regions. With CRR, every object uploaded to an S3 bucket is automatically replicated to a destination bucket in a different AWS Region that you choose, this enables you to copy the existing data across to each region - AMIs of both Amazon EBS-backed AMIs and instance store-backed AMIs can be copied between regions. You can then use the copied AMI to create a new launch configuration (remember that you cannot modify an ASG launch configuration, you must create a new launch configuration) There's no such thing as Multi-AZ for an S3 bucket (it's an RDS concept) Changing permissions on an AMI doesn't make it usable from another region, the AMI needs to be present within each region to be used. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

Q39)

An application hosted in your VPC uses an EC2 instance with a MySQL DB running on it. The database uses a single 1TB General Purpose SSD (GP2) EBS volume. Recently it has been noticed that the database is not performing well and you need to improve the read performance.

What are two possible ways this can be achieved? (choose 2)

● Add an RDS read replica in another AZ

✓ Use a provisioned IOPS volume and specify the number of I/O operations required

Explanation:-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 SSD, Provisioned IOPS – I01 provides higher performance than General Purpose SSD (GP2) and you can specify the IOPS required up to 50 IOPS per GB and a maximum of 32000 IOPS RDS read replicas cannot be created from EC2 instances Creating an active/passive cluster doesn't improve read performance as the passive node is not servicing requests. This is use for fault tolerance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

● Add multiple EBS volumes in a RAID 1 array

✓ Add multiple EBS volumes in a RAID 0 array

Explanation:-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 SSD, Provisioned IOPS – I01 provides higher performance than General Purpose SSD (GP2) and you can specify the IOPS required up to 50 IOPS per GB and a maximum of 32000 IOPS RDS read replicas cannot be created from EC2 instances Creating an active/passive cluster doesn't improve read performance as the passive node is not servicing requests. This is use for fault tolerance. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

Q40)

Your company is reviewing their information security processes. One of the items that came out of a recent audit is that there is insufficient data recorded about requests made to a few S3 buckets. The security team requires an audit trail for operations on the S3 buckets that includes the requester, bucket name, request time, request action, and response status.

Which action would you take to enable this logging?

✓ Enable server access logging for the S3 buckets to save access logs to a specified destination bucket

Explanation:-Server access logging provides detailed records for the requests that are made to a bucket. To track requests for access to your bucket, you can enable server access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and an error code, if relevant For capturing IAM/user identity information in logs you would need to configure AWS CloudTrail Data Events (however this does not audit the bucket operations required in the question) Amazon S3 event notifications can be sent in response to actions in Amazon S3 like PUTs, POSTs, COPYs, or DELETEs.S3 event notifications records the request action but not the other requirements of the security team CloudWatch metrics do not include the bucket operations specified in the question References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/ https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html

● Enable S3 event notifications for the specific actions and setup an SNS notification

● Create a CloudTrail trail that audits S3 bucket operations

● Create a CloudWatch metric that monitors the S3 bucket operations and triggers an alarm

---

Q41) A colleague has asked you some questions about how AWS charge for DynamoDB. He is interested in knowing what type of workload DynamoDB is best suited for in relation to cost and how AWS charges for DynamoDB? (choose 2)

● You provision for expected throughput but are only charged for what you use

✓ Priced based on provisioned throughput (read/write) regardless of whether you use it or not

Explanation:-DynamoDB charges: - DynamoDB is more cost effective for read heavy workloads - It is priced based on provisioned throughput (read/write) regardless of whether you use it or not NOTE: With the DynamoDB Auto Scaling feature you can now have DynamoDB dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. However, this is relatively new and may not yet feature on the exam. See the link below for more details References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/ https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

● DynamoDB is more cost effective for write heavy workloads

✓ DynamoDB is more cost effective for read heavy workloads

Explanation:-DynamoDB charges: - DynamoDB is more cost effective for read heavy workloads - It is priced based on provisioned throughput (read/write) regardless of whether you use it or not NOTE: With the DynamoDB Auto Scaling feature you can now have DynamoDB dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. However, this is relatively new and may not yet feature on the exam. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/ https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

---

Q42)

You are a Solutions Architect at Digital Cloud Training. One of your clients runs an application that writes data to a DynamoDB

table. The client has asked how they can implement a function that runs code in response to item level changes that take place in the DynamoDB table.

What would you suggest to the client?

● Create a local secondary index that records item level changes and write some custom code that responds to updates to the index

✓ Enable DynamoDB Streams and create an event source mapping between AWS Lambda and the relevant stream

Explanation:-DynamoDB Streams help you to keep a list of item level changes or provide a list of item level changes that have taken place in the last 24hrs. Amazon DynamoDB is integrated with AWS Lambda so that you can create triggers—pieces of code that automatically respond to events in DynamoDB Streams If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records An event source mapping identifies a poll-based event source for a Lambda function. It can be either an Amazon Kinesis or DynamoDB stream. Event sources maintain the mapping configuration except for stream-based services (e.g. DynamoDB, Kinesis) for which the configuration is made on the Lambda side and Lambda performs the polling You cannot configure DynamoDB as a Kinesis Data Streams producer You can write Lambda functions to process S3 bucket events, such as the object-created or object-deleted events. For example, when a user uploads a photo to a bucket, you might want Amazon S3 to invoke your Lambda function so that it reads the image and creates a thumbnail for the photo . However, the questions asks for a solution that runs code in response to changes in a DynamoDB table, not an S3 bucket A local secondary index maintains an alternate sort key for a given partition key value, it does not record item level changes References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/ https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/

● Enable server access logging and create an event source mapping between AWS Lambda and the S3 bucket to which the logs are written

● Use Kinesis Data Streams and configure DynamoDB as a producer

Q43)

Your company is starting to use AWS to host new web-based applications. A new two-tier application will be deployed that provides customers with access to data records. It is important that the application is highly responsive and retrieval times are optimized. You're looking for a persistent data store that can provide the required performance.

From the list below what AWS service would you recommend for this requirement?

● Kinesis Data Streams

✓ ElastiCache with the Redis engine

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 There are two different database engines with different characteristics as per below: Memcached - Not persistent - Cannot be used as a data store - Supports large nodes with multiple cores or threads - Scales out and in, by adding and removing nodes Redis - Data is persistent - Can be used as a datastore - Not multi-threaded - Scales by adding shards, not nodes Kinesis Data Streams is used for processing streams of data, it is not a persistent data store RDS is not the optimum solution due to the requirement to optimize retrieval times which is a better fit for an in-memory data store such as ElastiCache References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/

● ElastiCache with the Memcached engine

● RDS in a multi-AZ configuration

Q44)

You are a Solutions Architect at Digital Cloud Training. A client from a large multinational corporation is working on a deployment of a significant amount of resources into AWS. The client would like to be able to deploy resources across multiple AWS accounts and regions using a single toolset and template.

You have been asked to suggest a toolset that can provide this functionality?

● Use a third-party product such as Terraform that has support for multiple AWS accounts and regions

✓ Use a CloudFormation StackSet and specify the target accounts and regions in which the stacks will be created

Explanation:-AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified regions. An administrator account is the AWS account in which you create stack sets A stack set is managed by signing in to the AWS administrator account in which it was created. A target account is the account into which you create, update, or delete one or more stacks in your stack set Before you can use a stack set to create stacks in a target account, you must set up a trust relationship between the administrator and target accounts A regular CloudFormation template cannot be used across regions and accounts. You would need to create copies of the template and then manage updates You do not need to use a third-party product such as Terraform as this functionality can be delivered through native AWS technology References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/ https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-concepts.html

● Use a CloudFormation template that creates a stack and specify the logical IDs of each account and region

● This cannot be done, use separate CloudFormation templates per AWS account and region

Q45)

Your client is looking for a fully managed directory service in the AWS cloud. The service should provide an inexpensive Active Directory-compatible service with common directory features. The client is a medium-sized organization with 4000 users.

As the client has a very limited budget it is important to select a cost-effective solution.What would you suggest?

✓ AWS Simple AD

Explanation:-Simple AD is an inexpensive Active Directory-compatible service with common directory features. It is a standalone, fully managed, directory on the AWS cloud and is generally the least expensive option. It is the best choice for less than 5000 users and when you don't need advanced AD features 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. It provides advanced AD features that you don't get with SimpleAD Amazon Cognito is an authentication service for web and mobile apps AWS Single Sign-On (SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

● AWS Active Directory Service for Microsoft Active Directory
● Amazon Cognito
● AWS Single Sign-On

Q46)

You have been asked to implement a solution for capturing, transforming and loading streaming data into an Amazon RedShift cluster. The solution will capture data from Amazon Kinesis Data Streams.

Which AWS services would you utilize in this scenario? (choose 2)

● EMR for transforming the data
✓ Lambda for transforming the data

Explanation:-For this solution Kinesis Data Firehose can be used as it can use Kinesis Data Streams as a source and can capture, transform, and load streaming data into a RedShift cluster. Kinesis Data Firehose can invoke a Lambda function to transform data before delivering it to destinations Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing, this solution does not involve video streams AWS Data Pipeline is used for processing and moving data between compute and storage services. It does not work with streaming data as Kinesis does Elastic Map Reduce (EMR) is used for processing and analyzing data using the Hadoop framework. It is not used for transforming streaming data. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

● Kinesis Video Streams for capturing the data and loading it into RedShift
✓ Kinesis Data Firehose for capturing the data and loading it into RedShift

Explanation:-For this solution Kinesis Data Firehose can be used as it can use Kinesis Data Streams as a source and can capture, transform, and load streaming data into a RedShift cluster. Kinesis Data Firehose can invoke a Lambda function to transform data before delivering it to destinations Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing, this solution does not involve video streams AWS Data Pipeline is used for processing and moving data between compute and storage services. It does not work with streaming data as Kinesis does Elastic Map Reduce (EMR) is used for processing and analyzing data using the Hadoop framework. It is not used for transforming streaming data. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

Q47)

You are creating a design for a web-based application that will be based on a web front-end using EC2 instances and a database back-end. This application is a low priority and you do not want to incur costs in general day to day management.

Which AWS database service can you use that will require the least operational overhead?

● RDS
● RedShift
● EMR
✓ DynamoDB

Explanation:-Out of the options in the list, DynamoDB requires the least operational overhead as there are no backups, maintenance periods, software updates etc. to deal with RDS, RedShift and EMR all require some operational overhead to deal with backups, software updates and maintenance periods References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

Q48)

A new Big Data application you are developing will use hundreds of EC2 instances to write data to a shared file system. The file system must be stored redundantly across multiple AZs within a region and allow the EC2 instances to concurrently access the file system. The required throughput is multiple GB per second.

From the options presented which storage solution can deliver these requirements?

✓ Amazon EFS

Explanation:-Amazon EFS is the best solution as it is the only solution that is a file-level storage solution (not block/object-based), stores data redundantly across multiple AZs within a region and you can concurrently connect up to thousands of EC2 instances to a single filesystem Amazon EBS volumes cannot be accessed by concurrently by multiple instances Amazon S3 is an object store, not a file system Amazon Storage Gateway is a range of products used for on-premises storage management and can be configured to cache data locally, backup data to the cloud and also provides a virtual tape backup solution References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

● Amazon EBS using multiple volumes in a RAID 0 configuration
● Amazon S3
● Amazon Storage Gateway

Q49) A company has deployed Amazon RedShift for performing analytics on user data. When using Amazon RedShift, which of the following statements are correct in relation to availability and durability? (choose 2)

✓ RedShift provides continuous/incremental backups

Explanation:-RedShift always keeps three copies of your data and provides continuous/incremental backups Corrections: Single-node clusters do not support data replication Manual backups are not automatically deleted when you delete a cluster References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

● Single-node clusters support data replication
✓ RedShift always keeps three copies of your data

Explanation:-RedShift always keeps three copies of your data and provides continuous/incremental backups Corrections: Single-node clusters do not support data replication Manual backups are not automatically deleted when you delete a cluster References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

● RedShift always keeps five copies of your data

Q50)

You are planning to launch a RedShift cluster for processing and analyzing a large amount of data. The RedShift cluster will be deployed into a VPC with multiple subnets.

Which construct is used when provisioning the cluster to allow you to specify a set of subnets in the VPC that the cluster will be deployed into?

● DB Subnet Group
● Subnet Group
● Availability Zone (AZ)
✓ Cluster Subnet Group

Explanation:-You create a cluster subnet group if you are provisioning your cluster in your virtual private cloud (VPC) A cluster subnet group allows you to specify a set of subnets in your VPC When provisioning a cluster you provide the subnet group and Amazon Redshift creates the cluster on one of the subnets in the group A DB Subnet Group is used by RDS A Subnet Group is used by ElastiCache Availability Zones are part of the AWS global infrastructure, subnets reside within AZs but in RedShift you provision the cluster into Cluster Subnet Groups. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/ https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-cluster-subnet-groups.html