Answer Sheet

Q1)

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?

- Sticky Sessions
- ✅ 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/

- Deletion Protection
- Proxy Protocol

Q2)

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?

- DynamoDB with Global Tables
- ✅ 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/

- EC2 instances with EBS replication
- RDS with Multi-AZ

Q3)

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 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/

- Install a Microsoft Active Directory Domain Controller on AWS and add it into your existing on-premise domain
- Launch a large AWS Directory Service AD Connector to proxy all authentication back to your on-premise AD service for authentication
- Use a large AWS Simple AD in AWS

Q4)

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?

- ✅ 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

- Resources
- Mappings
- Parameters

Q5) 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 AWS Import/Export
- ✅ 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 a single PUT request to upload the large file
- Use Amazon Snowball

Q6)

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?

- On-demand 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/

- Spot instances
- Flexible instances

Q7)

A company needs to deploy virtual desktops for its customers in an AWS VPC and would like to leverage their existing on-premise security principals. AWS Workspaces will be used as the virtual desktop solution.

Which set of AWS services and features will meet the company's requirements?

- A VPN connection, VPC NACLs and Security Groups
- ✅ A VPN connection, and AWS Directory Services

Explanation:-A security principle is a-crum_add_start--->

- AWS Directory Service and AWS IAM
- Amazon EC2, and AWS IAM

Q8)

You have an application running in ap-southeast that requires six EC2 instances running at all times.

With three Availability Zones available in that region (ap-southeast-2a, ap-southeast-2b, and ap-southeast-2c), which of the following deployments provides fault tolerance if any single Availability Zone in ap-southeast-2 becomes unavailable? (choose 2)

- 3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c
- 2 EC2 instances in ap-southeast-2a, 2 EC2 instances in ap-southeast-2b, 2 EC2 instances in ap-southeast-2c
- ✅ 6 EC2 instances in ap-southeast-2a, 6 EC2 instances in ap-southeast-2b, no EC2 instances in ap-southeast-2c

Explanation:-This is a simple mathematical problem. Take note that the question asks that 6 instances must be available in the event that ANY SINGLE AZ becomes unavailable. There are only 2 options that fulfil these criteria 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/

- ✅ 3 EC2 instances in ap-southeast-2a, 3 EC2 instances in ap-southeast-2b, 3 EC2 instances in ap-southeast-2c

Explanation:-This is a simple mathematical problem. Take note that the question asks that 6 instances must be available in the event that ANY SINGLE AZ becomes unavailable. There are only 2 options that fulfil these criteria 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/

Q9)

A major upcoming sales event is likely to result in heavy read traffic to a web application your company manages. As the Solutions Architect you have been asked for advice on how best to protect the database tier from the heavy load and ensure the user experience is not impacted.

The web application owner has also requested that the design be fault tolerant. The current configuration consists of a web application behind an ELB that uses Auto Scaling and an RDS MySQL database running in a multi-AZ configuration. As the database load is highly changeable the solution should allow elasticity by adding and removing nodes as required and should also be multi-threaded.

What recommendations would you make?

- Deploy an ElastiCache Redis cluster with cluster mode disabled and multi-AZ with automatic failover
- Deploy an ElastiCache Memcached cluster in multi-AZ mode in the same AZs as RDS
- ✅ Deploy an ElastiCache Memcached cluster in both AZs in which the RDS database is deployed

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 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 References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/ https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/SelectEngine.html

- Deploy an ElastiCache Redis cluster with cluster mode enabled and multi-AZ with automatic failover

---

Q10)

An EC2 instance in an Auto Scaling group that has been reported as unhealthy has been marked for replacement.

What is the process Auto Scaling uses to replace the instance? (choose 2)

- Auto Scaling has to perform rebalancing first, and then terminate the instance
- Auto Scaling has to launch a replacement first before it can terminate the unhealthy instance
- ✅ If connection draining is enabled, Auto Scaling will wait for in-flight connections to complete or timeout

Explanation:-If connection draining is enabled, Auto Scaling waits for in-flight requests to complete or timeout before terminating instances. Auto Scaling will terminate the existing instance before launching a replacement instance Auto Scaling does not send a notification to the administrator Unlike AZ rebalancing, termination of unhealthy instances happens first, then Auto Scaling attempts to launch new instances to replace terminated instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- ✅ Auto Scaling will terminate the existing instance before launching a replacement instance

Explanation:-If connection draining is enabled, Auto Scaling waits for in-flight requests to complete or timeout before terminating instances. Auto Scaling will terminate the existing instance before launching a replacement instance Auto Scaling does not send a notification to the administrator Unlike AZ rebalancing, termination of unhealthy instances happens first, then Auto Scaling attempts to launch new instances to replace terminated instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

Q11)

A Solutions Architect is determining the best method for provisioning Internet connectivity for a data-processing application that will pull large amounts of data from an object storage system via the Internet. The solution must be redundant and have no constraints on bandwidth.

Which option satisfies these requirements?

- ✅ Attach an Internet Gateway

Explanation:-Both a NAT gateway and an Internet gateway offer redundancy however the NAT gateway is limited to 45 Gbps whereas the IGW does not impose any limits A VPC endpoint is used to access public services from a VPC without traversing the Internet NAT instances are EC2 instances that are used, in a similar way to NAT gateways, by instances in private subnets to access the Internet. However they are not redundant and are limited in bandwidth References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Create a VPC endpoint
- Deploy NAT Instances in a public subnet
- Use a NAT Gateway

Q12)

For security reasons, you need to ensure that an On-Demand EC2 instance can only be accessed from a specific public IP address (100.156.52.12) using the SSH protocol. You are configuring the Security Group of the EC2 instance, and need to configure an Inbound rule.

Which of the rules below will achieve the requirement?

- Protocol - UDP, Port Range - 22, Source 100.156.52.12/0
- Protocol - UDP, Port Range - 22, Source 100.156.52.12/32
- Protocol - TCP, Port Range - 22, Source 100.156.52.12/0
- ✅ Protocol - TCP, Port Range - 22, Source 100.156.52.12/32

Explanation:-The SSH protocol uses TCP port 22 and to specify an individual IP address in a security group rule you use the format X.X.X.X/32. Therefore the rule should allow TCP port 22 from 100.156.52.12/32 Security groups act like a firewall at the instance level. Specifically, security groups operate at the network interface level and you can only assign permit rules in a security group, you cannot assign a deny rule References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q13)

A company is migrating an on-premises 10 TB MySQL database to AWS. The company expects the database to quadruple in size and the business requirement is that replicate lag must be kept under 100 milliseconds.

Which Amazon RDS engine meets these requirements?

- Microsoft SQL Server
- ✅ Amazon Aurora

Explanation:-Aurora databases can scale up to 64 TB and Aurora replicas features millisecond latency All other RDS engines have a limit of 16 TiB maximum DB size and asynchronous replication typically takes seconds References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/ https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_Limits.html

- Oracle
- MySQL

Q14)

A Solutions Architect is designing a solution for a financial application that will receive trading data in large volumes.

What is the best solution for ingesting and processing a very large number of data streams in near real time?

- RedShift
- ✅ Kinesis Data Streams

Explanation:-Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. It enables real-time processing of streaming big data and can be used for rapidly moving data off data producers and then continuously processing the data. Kinesis Data Streams stores data for later processing by applications (key difference with Firehose which delivers data directly to AWS services) Kinesis Firehose can allow transformation of data and it then delivers data to supported services RedShift is a data warehouse solution used for analyzing data EMR is a hosted Hadoop framework that is used for analytics References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

- Kinesis Firehose
- EMR

Q15)

You are creating a design for an internal-only AWS service that uses EC2 instances to process information on S3 and store the results in DynamoDB. You need to allow access to several developers who will be testing code and need to apply security best practices to the architecture.

Which of the security practices below are recommended? (choose 2)

- Store the access keys and secret IDs within the application
- Assign an IAM user for each EC2 instance
- ✅ Use bastion hosts to enforce control and visibility

Explanation:-Best practices for securing operating systems and applications include: Disable root API access keys and secret key Restrict access to instances from limited IP ranges using Security Groups Password protect the .pem file on user machines Delete keys from the authorized_keys file on your instances when someone leaves your organization or no longer requires access Rotate credentials (DB, Access Keys) Regularly run least privilege checks using IAM user Access Advisor and IAM user Last Used Access Keys Use bastion hosts to enforce control and visibility References: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

- ✅ Disable root API access keys and secret key

Explanation:-Best practices for securing operating systems and applications include: Disable root API access keys and secret key Restrict access to instances from limited IP ranges using Security Groups Password protect the .pem file on user machines Delete keys from the authorized_keys file on your instances when someone leaves your organization or no longer requires access Rotate credentials (DB, Access Keys) Regularly run least privilege checks using IAM user Access Advisor and IAM user Last Used Access Keys Use bastion hosts to enforce control and visibility References: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

---

Q16) You have an unhealthy EC2 instance attached to an ELB that is being taken out of service. While the EC2 instance is being de-registered from the ELB, which ELB feature will cause the ELB to stop sending any new requests to the EC2 instance whilst allowing in-flight sessions to complete?

- ✅ ELB 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?? Cross-zone load balancing is used to enable equal distribution of connections to targets in multiple AZs Session affinity enables the load balancer to bind a user's session to a specific instance Proxy Protocol is an Internet protocol used to carry connection information from the source requesting the connection to the destination for which the connection was requested References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- ELB session affinity (sticky session)
- ELB proxy protocol
- ELB Cross zone load balancing

Q17)

A Solutions Architect is designing a static website that will use the zone apex of a DNS domain (e.g. example.com). The Architect wants to use the Amazon Route 53 service.

Which steps should the Architect take to implement a scalable and cost-effective solution? (choose 2)

- ✅ Create a Route 53 hosted zone, and set the NS records of the domain to use Route 53 name servers

Explanation:-To use Route 53 for an existing domain the Architect needs to change the NS records to point to the Amazon Route 53 name servers. This will direct name resolution to Route 53 for the domain name. The most cost-effective solution for hosting the website will be to use an Amazon S3 bucket. To do this you create a bucket using the same name as the domain name (e.g. example.com) and use a Route 53 Alias record to map to it Using an EC2 instance instead of an S3 bucket would be more costly so that rules out 2 options that explicitly mention EC3 Elastic Beanstalk provisions EC2 instances so again this would be a more costly option References: https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html

- Host the website on an Amazon EC2 instance, and map a Route 53 Alias record to the public IP address of the EC2 instance

- Host the website using AWS Elastic Beanstalk, and map a Route 53 Alias record to the Beanstalk stack
- ✅ Serve the website from an Amazon S3 bucket, and map a Route 53 Alias record to the website endpoint

Explanation:-To use Route 53 for an existing domain the Architect needs to change the NS records to point to the Amazon Route 53 name servers. This will direct name resolution to Route 53 for the domain name. The most cost-effective solution for hosting the website will be to use an Amazon S3 bucket. To do this you create a bucket using the same name as the domain name (e.g. example.com) and use a Route 53 Alias record to map to it Using an EC2 instance instead of an S3 bucket would be more costly so that rules out 2 options that explicitly mention EC3 Elastic Beanstalk provisions EC2 instances so again this would be a more costly option References: https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html

---

Q18) You have been asked to design a cloud-native application architecture using AWS services. What is a typical use case for SQS?

- Sending emails to clients when a job is completed
- Co-ordination of work items between different human and non-human workers
- Providing fault tolerance for S3
- ✅ Decoupling application components to ensure that there is no dependency on the availability of a single component

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. SQS is used for distributed/decoupled applications and can be used with RedShift, DynamoDB, EC2, ECS, RDS, S3 and Lambda SQS cannot be used for providing fault tolerance for S3 as messages can only be stored in the queue for a maximum amount of time Simple Workflow Service (SWF) is used for co-ordination of work items between different human and non-human workers Simple Notification Service (SNS) can be used for sending email notifications when certain events happen References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/

Q19)

There is expected to be a large increase in write intensive traffic to a website you manage that registers users onto an online learning program. You are concerned about writes to the database being dropped and need to come up with a solution to ensure this does not happen.

Which of the solution options below would be the best approach to take?

- Use RDS in a multi-AZ configuration to distribute writes across AZs
- Update the application to write data to an S3 bucket and provision additional EC2 instances to process the data and write it to the database
- Use CloudFront to cache the writes and configure the database as a custom origin
- ✅ Update the application to write data to an SQS queue and provision additional EC2 instances to process the data and write it to the database

Explanation:-This is a great use case for Amazon Simple Queue Service (Amazon SQS). SQS is a web service that gives you access to message queues that store messages waiting to be processed and offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers. SQS is used for distributed/decoupled applications. In this circumstance SQS will reduce the risk of writes being dropped and it the best option presented RDS in a multi-AZ configuration will not help as writes are only made to the primary database Though writing data to an S3 bucket could potentially work, it is not the best option as SQS is recommended for decoupling application components The CloudFront option is bogus as you cannot configure a database as a custom origin in CloudFront References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/

Q20)

A Solutions Architect has been asked to improve the performance of a DynamoDB table. Latency is currently a few milliseconds and this needs to be reduced to microseconds whilst also scaling to millions of requests per second.

What is the BEST architecture to support this?

- ✅ Create a DynamoDB Accelerator (DAX) cluster

Explanation:-Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second It is possible to use ElastiCache in front of DynamoDB, however this is not a supported architecture DynamoDB is not a supported origin for CloudFront Reducing the number of Scan operations on DynamoDB may improve performance but will not reduce latency to microseconds References: https://aws.amazon.com/dynamodb/dax/

- Reduce the number of Scan operations
- Use CloudFront to cache the content
- Create an ElastiCache Redis cluster

Q21)

You work for Digital Cloud Training and have just created a number of IAM users in your AWS account. You need to ensure that the users are able to make API calls to AWS services.

What else needs to be done?

- Create a group and add the users to it
- Enable Multi-Factor Authentication for the users
- ✅ Create a set of Access Keys for the users

Explanation:-Access keys are a combination of an access key ID and a secret access key and you can assign two active access keys to a user at a time. These can be used to make programmatic calls to AWS when using the API in program code or at a command prompt when using the AWS CLI or the AWS PowerShell tools A password is needed for logging into the console but not for making API calls to AWS services. Similarly you don't need to create a group and add the users to it to provide access to make API calls to AWS services Multi-factor authentication can be used to control access to AWS service APIs but the question is not asking how to better secure the calls but just being able to make them References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

- Set a password for each user

Q22)

You are a Solutions Architect at Digital Cloud Training. One of your clients is an online media company that attracts a large volume of users to their website each day. The media company are interested in analyzing the user's clickstream data so they can analyze user behavior in real-time and dynamically update advertising. This intelligent approach to advertising should help them to increase conversions.

What would you suggest as a solution to assist them with capturing and analyzing this data?

- Update the application to write data to an SQS queue, and create an additional application component to analyze the data in the queue and update the website
- Use EMR to process and analyze the data in real-time and Lambda to update the website based on the results
- Write the data directly to RedShift and use Business Intelligence tools to analyze the data
- ✅ Use Kinesis Data Streams to process and analyze the clickstream data. Store the results in DynamoDB and create an application component that reads the data from the database and updates the website

Explanation:-This is an ideal use case for Kinesis Data Streams which can process and analyze the clickstream data. Kinesis Data Streams stores the results in a number of supported services which includes DynamoDB SQS does not provide a solution for analyzing the data RedShift is a data warehouse and good for analytics on structured data. It is not used for real time ingestion EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3 and is used for processing large quantities of data. It is not suitable for this solution References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

Q23)

A company runs a multi-tier application in an Amazon VPC. The application has an ELB Classic Load Balancer as the front end in a public subnet, and an Amazon EC2-based reverse proxy that performs content-based routing to two back end EC2 instances in a

private subnet. The application is experiencing increasing load and the Solutions Architect is concerned that the reverse proxy and current back end setup will be insufficient.

Which actions should the Architect take to achieve a cost-effective solution that ensures the application automatically scales to meet the demand? (choose 2)

- Replace the Amazon EC2 reverse proxy with an ELB internal Classic Load Balancer
- Add Auto Scaling to the Amazon EC2 reverse proxy layer
- ✅ Add Auto Scaling to the Amazon EC2 back end fleet

Explanation:-Due to the reverse proxy being a bottleneck to scalability, we need to replace it with a solution that can perform content-based routing. This means we must use an ALB not a CLB as ALBs support path-based and host-based routing Auto Scaling should be added to the architecture so that the back end EC2 instances do not become a bottleneck. With Auto Scaling instances can be added and removed from the back end fleet as demand changes A Classic Load Balancer cannot perform content-based routing so cannot be used It is unknown how the reverse proxy can be scaled with Auto Scaling however using an ALB with content-based routing is a much better design as it scales automatically and is HA by default Burstable performance instances, which are T3 and T2 instances, are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload. CPU performance is not the constraint here and this would not be a cost-effective solution References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- ✅ Replace both the front end and reverse proxy layers with an Application Load Balancer

Explanation:-Due to the reverse proxy being a bottleneck to scalability, we need to replace it with a solution that can perform content-based routing. This means we must use an ALB not a CLB as ALBs support path-based and host-based routing Auto Scaling should be added to the architecture so that the back end EC2 instances do not become a bottleneck. With Auto Scaling instances can be added and removed from the back end fleet as demand changes A Classic Load Balancer cannot perform content-based routing so cannot be used It is unknown how the reverse proxy can be scaled with Auto Scaling however using an ALB with content-based routing is a much better design as it scales automatically and is HA by default Burstable performance instances, which are T3 and T2 instances, are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload. CPU performance is not the constraint here and this would not be a cost-effective solution References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

Q24)

Your company has an on-premise LDAP directory service. As part of a gradual migration into AWS you would like to integrate the LDAP directory with AWS's Identity and Access Management (IAM) solutions so that existing users can authenticate against AWS services.

What method would you suggest using to enable this integration?

- Use SAML to develop a direct integration from the on-premise LDAP directory to the relevant AWS services
- Create a policy in IAM that references users in the on-premise LDAP directory
- Use AWS Simple AD and create a trust relationship with IAM
- ✅ Develop an on-premise custom identity provider (IdP) and use the AWS Security Token Service (STS) to provide temporary security credentials

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). If your identity store is not compatible with SAML 2.0, then you can build a custom identity broker application to perform a similar function. The broker application authenticates users, requests temporary credentials for users from AWS, and then provides them to the user to access AWS resources You cannot create trust relationships between SimpleAD and IAM You cannot use references in an IAM policy to an on-premise AD SAML may not be supported by the on-premise LDAP directory so you would need to develop a custom IdP and use STS References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/ https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html

---

Q25)

Your company currently uses Puppet Enterprise for infrastructure and application management. You are looking to move some of your infrastructure onto AWS and would like to continue to use the same tools in the cloud.

What AWS service provides a fully managed configuration management service that is compatible with Puppet Enterprise?

- Elastic Beanstalk
- CloudFormation
- ✅ OpsWorks

Explanation:-The only service that would allow you to continue to use the same tools is OpsWorks. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-opsworks/ https://docs.aws.amazon.com/opsworks/latest/userguide/welcome.html

- CloudTrail

Q26)

You manage an application that uses Auto Scaling. Recently there have been incidents of multiple scaling events in an hour and you are looking at methods of stabilising the Auto Scaling Group.

Select the statements below that are correct with regards to the Auto Scaling cooldown period? (choose 2)

- It ensures that before the Auto Scaling group scales out, the EC2 instances can apply system updates
- ✅ The default value is 300 seconds

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 The default cooldown period is applied when you create your Auto Scaling group The default value is 300 seconds You can configure the default cooldown period when you create the Auto Scaling group, using the AWS Management Console, the create-auto-scaling-group command (AWS CLI), or the CreateAutoScalingGroup API operation References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://docs.aws.amazon.com/autoscaling/ec2/userguide/Cooldown.html

- ✅ It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect

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 The default cooldown period is applied when you create your Auto Scaling group The default value is 300 seconds You can configure the default cooldown period when you create the Auto Scaling group, using the AWS Management Console, the create-auto-scaling-group command (AWS CLI), or the CreateAutoScalingGroup API operation References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://docs.aws.amazon.com/autoscaling/ec2/userguide/Cooldown.html

- It ensures that the Auto Scaling group terminates the EC2 instances that are least busy

---

Q27)

Your Systems Administrators currently use Chef for configuration management of on-premise servers.

Which AWS service will provision a fully-managed Chef server and allow you to use your existing Chef cookbooks and recipes?

- CloudFormation
- Opsworks Stacks
- ✅ OpsWorks for Chef Automate

Explanation:-AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. AWS OpsWorks for Chef Automate is a fully-managed configuration management service that hosts Chef Automate, a suite of automation tools from Chef for configuration management, compliance and security, and continuous deployment. OpsWorks for Chef Automate is completely compatible with tooling and cookbooks from the Chef community and automatically registers new nodes with your Chef server The OpsWorks Stacks service helps you model, provision, and

manage your applications on AWS using the embedded Chef solo client that is installed on Amazon EC2 instances on your behalf Elastic Beanstalk and CloudFormation are not able to build infrastructure using Chef cookbooks References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-opsworks/

- Elastic Beanstalk

Q28)

You have created a new VPC and setup an Auto Scaling Group to maintain a desired count of 2 EC2 instances. The security team has requested that the EC2 instances be located in a private subnet. To distribute load, you have to also setup an Internet-facing Application Load Balancer (ALB).

With your security team's wishes in mind what else needs to be done to get this configuration to work? (choose 2)

- ✅ Associate the public subnets with the ALB

Explanation:-ELB nodes have public IPs and route traffic to the private IP addresses of the EC2 instances. You need one public subnet in each AZ where the ELB is defined and the private subnets are located Attaching an Internet gateway (which is done at the VPC level, not the subnet level) or a NAT gateway will not assist as these are both used for outbound communications which is not the goal here ELBs talk to the private IP addresses of the EC2 instances so adding an Elastic IP address to the instance won't help. Additionally Elastic IP addresses are used in public subnets to allow Internet access via an Internet Gateway References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

- Attach an Internet Gateway to the private subnets
- Add a NAT gateway to the private subnet
- ✅ For each private subnet create a corresponding public subnet in the same AZ

Explanation:-ELB nodes have public IPs and route traffic to the private IP addresses of the EC2 instances. You need one public subnet in each AZ where the ELB is defined and the private subnets are located Attaching an Internet gateway (which is done at the VPC level, not the subnet level) or a NAT gateway will not assist as these are both used for outbound communications which is not the goal here ELBs talk to the private IP addresses of the EC2 instances so adding an Elastic IP address to the instance won't help. Additionally Elastic IP addresses are used in public subnets to allow Internet access via an Internet Gateway References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

Q29) A Solutions Architect is creating a design for a multi-tiered serverless application. Which two services form the application facing services from the AWS serverless infrastructure? (choose 2)

- ✅ API Gateway

Explanation:-The only application services here are API Gateway and Lambda and these are considered to be serverless services ECS provides the platform for running containers and uses Amazon EC2 instances ELB provides distribution of incoming network connections and also uses Amazon EC2 instances AWS Cognito is used for providing authentication services for web and mobile apps References: https://aws.amazon.com/serverless/

- AWS Cognito
- ✅ AWS Lambda

Explanation:-The only application services here are API Gateway and Lambda and these are considered to be serverless services ECS provides the platform for running containers and uses Amazon EC2 instances ELB provides distribution of incoming network connections and also uses Amazon EC2 instances AWS Cognito is used for providing authentication services for web and mobile apps References: https://aws.amazon.com/serverless/

- Elastic Load Balancer

Q30)

A new security mandate requires that all personnel data held in the cloud is encrypted at rest.

Which two methods allow you to encrypt data stored in S3 buckets at rest cost-efficiently? (choose 2)

- Make use of AWS S3 bucket policies to control access to the data at rest
- ✅ Use AWS S3 server-side encryption with Key Management Service keys or Customer-provided keys

Explanation:-When using S3 encryption your data is always encrypted at rest and you can choose to use KMS managed keys or customer-provided keys. If you encrypt the data at the source and transfer it in an encrypted state it will also be encrypted in-transit With client side encryption data is encrypted on the client side and transferred in an encrypted state and with server-side encryption data is encrypted by S3 before it is written to disk (data is decrypted when it is downloaded) You can use bucket policies to control encryption of data that is uploaded but use of encryption is not stated in the answer given. Simply using bucket policies to control access to the data does not meet the security mandate that data must be encrypted Multipart upload helps with uploading large files but does not encrypt your data CloudHSM can be used to encrypt data but as a dedicated service it is charged on an hourly basis and is less cost-efficient compared to S3 encryption or encrypting the data at the source. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- ✅ Encrypt the data at the source using the client's CMK keys before transferring it to S3

Explanation:-When using S3 encryption your data is always encrypted at rest and you can choose to use KMS managed keys or customer-provided keys. If you encrypt the data at the source and transfer it in an encrypted state it will also be encrypted in-transit With client side encryption data is encrypted on the client side and transferred in an encrypted state and with server-side encryption data is encrypted by S3 before it is written to disk (data is decrypted when it is downloaded) You can use bucket policies to control encryption of data that is uploaded but use of encryption is not stated in the answer given. Simply using bucket policies to control access to the data does not meet the security mandate that data must be encrypted Multipart upload helps with uploading large files but does not encrypt your data CloudHSM can be used to encrypt data but as a dedicated service it is charged on an hourly basis and is less cost-efficient compared to S3 encryption or encrypting the data at the source. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Use CloudHSM

Q31)

You are configuring Route 53 for a customer's website. Their web servers are behind an Internet-facing ELB.

What record set would you create to point the customer's DNS zone apex record at the ELB?

- Create a CNAME record that is an Alias, and select the ELB DNS as a target
- Create an A record pointing to the DNS name of the load balancer
- ✅ Create an A record that is an Alias, and select the ELB DNS as a target

Explanation:-An Alias record can be used for resolving apex or naked domain names (e.g. example.com). You can create an A record that is an Alias that uses the customer's website zone apex domain name and map it to the ELB DNS name A CNAME record can't be used for resolving apex or naked domain names A standard A record maps the DNS domain name to the IP address of a resource. You cannot obtain the IP of the ELB so you must use an Alias record which maps the DNS domain name of the customer's website to the ELB DNS name (rather than its IP) PTR records are reverse lookup records where you use the IP to find the DNS name References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

- Create a PTR record pointing to the DNS name of the load balancer

---

Q32)

You are putting together a design for a web-facing application. The application will be run on EC2 instances behind ELBs in multiple regions in an active/passive configuration. The website address the application runs on is digitalcloud.guru. You will be using Route 53 to perform DNS resolution for the application.

How would you configure Route 53 in this scenario based on AWS best practices? (choose 2)

- ✅ Use a Failover Routing Policy

Explanation:-The failover routing policy is used for active/passive configurations. Alias records can be used to map the domain apex (digitalcloud.training) to the Elastic Load Balancers. Weighted routing is not an active/passive routing policy. All records are active and the traffic is distributed according to the weighting You cannot use CNAME records for the domain apex record, you must use Alias records When using the failover routing policy with Alias records

set Evaluate Target Health to “Yes?? and do not use health checks (set "Associate with Health Check" to "No") References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

- Connect the ELBs using CNAME records
- Use a Weighted Routing Policy
- ✅ Connect the ELBs using Alias records

Explanation:-The failover routing policy is used for active/passive configurations. Alias records can be used to map the domain apex (digitalcloud.training) to the Elastic Load Balancers. Weighted routing is not an active/passive routing policy. All records are active and the traffic is distributed according to the weighting You cannot use CNAME records for the domain apex record, you must use Alias records When using the failover routing policy with Alias records set Evaluate Target Health to “Yes?? and do not use health checks (set "Associate with Health Check" to "No") References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

Q33)

You need to create an EBS volume to mount to an existing EC2 instance for an application that will be writing structured data to the volume. The application vendor suggests that the performance of the disk should be up to 3 IOPS per GB. You expect the capacity of the volume to grow to 2TB.

Taking into account cost effectiveness, which EBS volume type would you select?

- Throughput Optimized HDD (ST1)
- ✅ General Purpose (GP2)

Explanation:-SSD, General Purpose (GP2) provides enough IOPS to support this requirement and is the most economical option that does. Using Provisioned IOPS would be more expensive and the other two options do not provide an SLA for IOPS More information on the volume types: - SSD, General Purpose (GP2) provides 3 IOPS per GB up to 16,000 IOPS. Volume size is 1 GB to 16 TB - Provisioned IOPS (Io1) provides the IOPS you assign up to 50 IOPS per GiB and up to 64,000 IOPS per volume. Volume size is 4 GB to 16TB - Throughput Optimized HDD (ST1) provides up to 500 IOPS per volume but does not provide an SLA for IOPS - Cold HDD (SC1) provides up to 250 IOPS per volume but does not provide an SLA for IOPS References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html?icmpid=docs_ec2_console

- Provisioned IOPS (IO1)
- Cold HDD (SC1)

Q34) A developer is writing some code and wants to work programmatically with IAM. Which feature of IAM allows you direct access to the IAM web service using HTTPS to call service actions and what is the method of authentication that must be used? (choose 2)

- OpenID Connect
- ✅ Access key ID and secret access key

Explanation:-AWS recommend that you use the AWS SDKs to make programmatic API calls to IAM. However, you can also use the IAM Query API to make direct calls to the IAM web service. An access key ID and secret access key must be used for authentication when using the Query API OpenID Connect is a provider for connecting external directories API gateway is a separate service for accepting and processing API calls An IAM role is not used for authentication to the Query API References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

- IAM role
- ✅ Query API

Explanation:-AWS recommend that you use the AWS SDKs to make programmatic API calls to IAM. However, you can also use the IAM Query API to make direct calls to the IAM web service. An access key ID and secret access key must be used for authentication when using the Query API OpenID Connect is a provider for connecting external directories API gateway is a separate service for accepting and processing API calls An IAM role is not used for authentication to the Query API References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

Q35)

A Solutions Architect is developing an application that will store and index large (>1 MB) JSON files. The data store must be highly available and latency must be consistently low even during times of heavy usage.

Which service should the Architect use?

- AWS CloudFormation
- DynamoDB
- Amazon RedShift
- ✅ Amazon EFS

Explanation:-EFS provides a highly-available data store with consistent low latencies and elasticity to scale as required RedShift is a data warehouse that is used for analyzing data using SQL DynamoDB is a low latency, highly available NoSQL DB. You can store JSON files up to 400KB in size in a DynamoDB table, for anything bigger you'd want to store a pointer to an object outside of the table CloudFormation is an orchestration tool and does not help with storing documents References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

Q36)

You have created an application in a VPC that uses a Network Load Balancer (NLB). The application will be offered in a service provider model for AWS principals in other accounts within the region to consume.

Based on this model, what AWS service will be used to offer the service for consumption?

- API Gateway
- ✅ VPC Endpoint Services using AWS PrivateLink

Explanation:-An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Route 53
- IAM Role Based Access Control

Q37) A critical database runs in your VPC for which availability is a concern. Which RDS DB instance events may force the DB to be taken offline during a maintenance window?

- ✅ Security patching

Explanation:-Maintenance windows are configured to allow DB instance modifications to take place such as scaling and software patching. Some operations require the DB instance to be taken offline brie

- Updating DB parameter groups
- Promoting a Read Replica
- Selecting the Multi-AZ feature

Q38)

The development team at your company have created a new mobile application that will be used by users to access confidential data. The developers have used Amazon Cognito for authentication, authorization, and user management. Due to the sensitivity of the data, there is a requirement to add another method of authentication in addition to a username and password.

You have been asked to recommend the best solution.

What is your recommendation?

- Enable multi-factor authentication (MFA) in IAM
- ✓ Use multi-factor authentication (MFA) with a Cognito user pool

Explanation:-You can use MFA with a Cognito user pool (not in IAM) and this satisfies the requirement. A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers Integrating IAM with a Cognito user pool or integrating a 3rd party IdP does not add another factor of authentication - "factors" include something you know (e.g. password), something you have (e.g. token device), and something you are (e.g. retina scan or fingerprint) References: https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-mfa.html

- Integrate IAM with a user pool in Cognito
- Integrate a third-party identity provider (IdP)

Q39)

You have been asked to recommend the best AWS storage solution for a client. The client requires a storage solution that provide a mounted file system for a Big Data and Analytics application. The client's requirements include high throughput, low latency, read-after-write consistency and the ability to burst up to multiple GB/s for short periods of time.

Which AWS service can meet this requirement?

- ✓ EFS

Explanation:-EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. EFS is good for big data and analytics, media processing workflows, content management, web serving, home directories etc.. EFS uses the NFSv4.1 protocol which is a protocol for mounting file systems (similar to Microsoft's SMB) EBS is mounted as a block device not a file system S3 is object storage DynamoDB is a fully managed NoSQL database References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

- DynamoDB
- EBS
- S3

Q40)

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)

- ✓ 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

- The database restore overwrites the existing database
- 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

---

Q41) Which of the following objects are good candidates to store in a cache? (Choose 3 answers)

- ✓ Session state

Explanation:-Many types of objects are good candidates to cache because they have the potential to be accessed by numerous users repeatedly. Even the balance of a bank account could be cached for short periods of time if the back-end database query is slow to respond.

- ✓ Shopping cart

Explanation:-Many types of objects are good candidates to cache because they have the potential to be accessed by numerous users repeatedly. Even the balance of a bank account could be cached for short periods of time if the back-end database query is slow to respond.

- ✓ Product catalog

Explanation:-Many types of objects are good candidates to cache because they have the potential to be accessed by numerous users repeatedly. Even the balance of a bank account could be cached for short periods of time if the back-end database query is slow to respond.

- Bank account balance

Q42) Which of the following cache engines are supported by Amazon ElastiCache? (Choose 2 answers)

- MySQL
- ✓ Memcached

Explanation:-Amazon ElastiCache supports Memcached and Redis cache engines. MySQL is not a cache engine, and Couchbase is not supported.

- ✓ Redis

Explanation:-Amazon ElastiCache supports Memcached and Redis cache engines. MySQL is not a cache engine, and Couchbase is not supported.

- Couchbase

Q43) How many nodes can you add to an Amazon ElastiCache cluster running Memcached?

- 1
- 5
- ✓ 20

Explanation:-The default limit is 20 nodes per cluster.

- 100

Q44) An application currently uses Memcached to cache frequently used database queries. Which steps are required to migrate the application to use Amazon ElastiCache with minimal changes? (Choose 2 answers)

- Recompile the application to use the Amazon ElastiCache libraries.
- ✓ Update the configuration file with the endpoint for the Amazon ElastiCache cluster.

Explanation:-Amazon ElastiCache is Application Programming Interface (API)-compatible with existing Memcached clients and does not require the application to be recompiled or linked against the libraries. Amazon ElastiCache manages the deployment of the Amazon ElastiCache binaries.

- ✓ Configure a security group to allow access from the application servers.

Explanation:-Amazon ElastiCache is Application Programming Interface (API)-compatible with existing Memcached clients and does not require the application to be recompiled or linked against the libraries. Amazon ElastiCache manages the deployment of the Amazon ElastiCache binaries.

- Connect to the Amazon ElastiCache nodes using Secure Shell (SSH) and install the latest version of Memcached.

Q45) How can you back up data stored in Amazon ElastiCache running Redis? (Choose 2 answers)

- Create an image of the Amazon Elastic Compute Cloud (Amazon EC2) instance.
- ✓ Configure automatic snapshots to back up the cache environment every night.

Explanation:-Amazon ElastiCache with the Redis engine allows for both manual and automatic snapshots. Memcached does not have a backup function.

- ✓ Create a snapshot manually.

Explanation:-Amazon ElastiCache with the Redis engine allows for both manual and automatic snapshots. Memcached does not have a backup function.

- Redis clusters cannot be backed up.

Q46) How can you secure an Amazon ElastiCache cluster? (Choose 3 answers)

- Change the Memcached root password.
- Restrict Application Programming Interface (API) actions using AWS Identity and Access Management (IAM) policies.

Explanation:-Limit access at the network level using security groups or network ACLs, and limit infrastructure changes using IAM.

- Restrict network access using security groups.

Explanation:-Limit access at the network level using security groups or network ACLs, and limit infrastructure changes using IAM.

- Restrict network access using a network Access Control List (ACL).

Explanation:-Limit access at the network level using security groups or network ACLs, and limit infrastructure changes using IAM.

Q47)

You are working on a mobile gaming application and are building the leaderboard feature to track the top scores across millions of users.

Which AWS services are best suited for this use case?

- Amazon Redshift
- Amazon ElastiCache using Memcached
- Amazon ElastiCache using Redis

Explanation:-Amazon ElastiCache with Redis provides native functions that simplify the development of leaderboards. With Memcached, it is more difficult to sort and rank large datasets. Amazon Redshift and Amazon S3 are not designed for high volumes of small reads and writes, typical of a mobile game.

- Amazon Simple Storage Service (S3)

Q48)

You have built a large web application that uses Amazon ElastiCache using Memcached to store frequent query results. You plan to expand both the web fleet and the cache fleet multiple times over the next year to accommodate increased user traffic.

How do you minimize the amount of changes required when a scaling event occurs?

- Configure AutoDiscovery on the client side

Explanation:-When the clients are configured to use AutoDiscovery, they can discover new cache nodes as they are added or removed. AutoDiscovery must be configured on each client and is not active server side. Updating the configuration file each time will be very difficult to manage. Using an Elastic Load Balancer is not recommended for this scenario.

- Configure AutoDiscovery on the server side
- Update the configuration file each time a new cluster
- Use an Elastic Load Balancer to proxy the requests

Q49) Which cache engines does Amazon ElastiCache support? (Choose 2 answers)

- Memcached

Explanation:-Amazon ElastiCache supports both Memcached and Redis. You can run self- managed installations of Membase and Couchbase using Amazon Elastic Compute Cloud

- Redis

Explanation:-Amazon ElastiCache supports both Memcached and Redis. You can run self- managed installations of Membase and Couchbase using Amazon Elastic Compute Cloud

- Membase
- Couchbase

Q50) What origin servers are supported by Amazon CloudFront? (Choose 3 answers)

- An Amazon Route 53 Hosted Zone
- An Amazon Simple Storage Service (Amazon S3) bucket

Explanation:-Amazon CloudFront can use an Amazon S3 bucket or any HTTP server, whether or not it is running in Amazon EC2. A Route 53 Hosted Zone is a set of DNS resource records, while an Auto Scaling Group launches or terminates Amazon EC2 instances automatically. Neither can be specified as an origin server for a distribution.

- An HTTP server running on Amazon Elastic Compute Cloud (Amazon EC2)

Explanation:-Amazon CloudFront can use an Amazon S3 bucket or any HTTP server, whether or not it is running in Amazon EC2. A Route 53 Hosted Zone is a set of DNS resource records, while an Auto Scaling Group launches or terminates Amazon EC2 instances automatically. Neither can be specified as an origin server for a distribution.

- An Amazon EC2 Auto Scaling Group
- An HTTP server running on-premises

Explanation:-Amazon CloudFront can use an Amazon S3 bucket or any HTTP server, whether or not it is running in Amazon EC2. A Route 53 Hosted Zone is a set of DNS resource records, while an Auto Scaling Group launches or terminates Amazon EC2 instances automatically. Neither can be specified as an origin server for a distribution.

Q51) Which of the following are good use cases for Amazon CloudFront? (Choose 2 answers)

- A popular software download site that supports users around the world, with dynamic content that changes rapidly

Explanation:-The site in A is “popular” and supports “users around the world,” key indicators that CloudFront is appropriate. Similarly, the site in C is “heavily used,” and requires private content, which is supported by Amazon CloudFront. Both B and D are corporate use cases where the requests come from a single geographic location or appear to come from one (because of the VPN). These use cases will generally not see benefit from Amazon CloudFront.

- A corporate website that serves training videos to employees. Most employees are located in two corporate campuses in the same city.
- A heavily used video and music streaming service that requires content to be delivered only to paid subscribers

Explanation:-The site in A is “popular” and supports “users around the world,” key indicators that CloudFront is appropriate. Similarly, the site in C is “heavily used,” and requires private content, which is supported by Amazon CloudFront. Both B and D are corporate use cases where the requests come from a single geographic location or appear to come from one (because of the VPN). These use cases will generally not see benefit from Amazon CloudFront.

- A corporate HR website that supports a global workforce. Because the site contains sensitive data, all users must connect through a corporate Virtual Private Network (VPN).

Q52)

You are building a media-sharing web application that serves video files to end users on both PCs and mobile devices. The media files are stored as objects in an Amazon Simple Storage Service (Amazon S3) bucket, but are to be delivered through Amazon CloudFront.

What is the simplest way to ensure that only Amazon CloudFront has access to the objects in the Amazon S3 bucket?

- Create Signed URLs for each Amazon S3 object.
- Use an Amazon CloudFront Origin Access Identifier (OAI).

Explanation:-Amazon CloudFront OAI is a special identity that can be used to restrict access to an Amazon S3 bucket only to an Amazon CloudFront distribution. Signed URLs, signed cookies, and IAM bucket policies can help to protect content served through Amazon CloudFront, but OAIs are the

simplest way to ensure that only Amazon CloudFront has access to a bucket.
- Use public and private keys with signed cookies.
- Use an AWS Identity and Access Management (IAM) bucket policy.

Q53)

Your company data center is completely full, but the sales group has determined a need to store 200TB of product video. The videos were created over the last several years, with the most recent being accessed by sales the most often. The data must be accessed locally, but there is no space in the data center to install local storage devices to store this data.

What AWS cloud service will meet sales' requirements?

- AWS Storage Gateway Gateway-Stored volumes
- Amazon Elastic Compute Cloud (Amazon EC2) instances with attached Amazon EBS Volumes
- ✅ AWS Storage Gateway Gateway-Cached volumes

Explanation:-AWS Storage Gateway allows you to access data in Amazon S3 locally, with the Gateway-Cached volume configuration allowing you to expand a relatively small amount of local storage into Amazon S3.

- AWS Import/Export Disk

Q54)

Your company wants to extend their existing Microsoft Active Directory capability into an Amazon Virtual Private Cloud (Amazon VPC) without establishing a trust relationship with the existing on-premises Active Directory.

Which of the following is the best approach to achieve this goal?

- Create and connect an AWS Directory Service AD Connector.
- ✅ Create and connect an AWS Directory Service Simple AD.

Explanation:-Simple AD is a Microsoft Active Directory-compatible directory that is powered by Samba 4. Simple AD supports commonly used Active Directory features such as user accounts, group memberships, domain-joining Amazon Elastic Compute Cloud (Amazon EC2) instances running Linux and Microsoft Windows, Kerberos-based Single Sign-On (SSO), and group policies.

- Create and connect an AWS Directory Service for Microsoft Active Directory (Enterprise Edition).
- None of the above

Q55) Which of the following are AWS Key Management Service (AWS KMS) keys that will never exit AWS unencrypted?

- AWS KMS data keys
- Envelope encryption keys
- ✅ AWS KMS Customer Master Keys (CMKs)

Explanation:-AWS KMS CMKs are the fundamental resources that AWS KMS manages. CMKs can never leave AWS KMS unencrypted, but data keys can.

- A and C

Q56) Which cryptographic method is used by AWS Key Management Service (AWS KMS) to encrypt data?

- Password-based encryption
- Asymmetric
- Shared secret
- ✅ Envelope encryption

Explanation:-AWS KMS uses envelope encryption to protect data. AWS KMS creates a data key, encrypts it under a Customer Master Key (CMK), and returns plaintext and encrypted versions of the data key to you. You use the plaintext key to encrypt data and store the encrypted key alongside the encrypted data. You can retrieve a plaintext data key only if you have the encrypted data key and you have permission to use the corresponding master key.

Q57) Which AWS service records Application Program Interface (API) calls made on your account and delivers log files to your Amazon Simple Storage Service (Amazon S3) bucket?

- ✅ AWS CloudTrail

Explanation:-AWS CloudTrail records important information about each API call, including the name of the API, the identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS Cloud service.

- Amazon CloudWatch
- Amazon Kinesis
- AWS Data Pipeline

Q58) You are trying to decrypt ciphertext with AWS KMS and the decryption operation is failing. Which of the following are possible causes? (Choose 2 answers)

- The private key does not match the public key in the ciphertext.
- ✅ The plaintext was encrypted along with an encryption context, and you are not providing the identical encryption context when calling the Decrypt API.

Explanation:-Encryption context is a set of key/value pairs that you can pass to AWS KMS when you call the Encrypt, Decrypt, ReEncrypt, GenerateDataKey, and GenerateDataKeyWithoutPlaintext APIs. Although the encryption context is not included in the ciphertext, it is cryptographically bound to the ciphertext during encryption and must be passed again when you call the Decrypt (or ReEncrypt) API. Invalid ciphertext for decryption is plaintext that has been encrypted in a different AWS account or ciphertext th

- ✅ The ciphertext you are trying to decrypt is not valid.

Explanation:-Encryption context is a set of key/value pairs that you can pass to AWS KMS when you call the Encrypt, Decrypt, ReEncrypt, GenerateDataKey, and GenerateDataKeyWithoutPlaintext APIs. Although the encryption context is not included in the ciphertext, it is cryptographically bound to the ciphertext during encryption and must be passed again when you call the Decrypt (or ReEncrypt) API. Invalid ciphertext for decryption is plaintext that has been encrypted in a different AWS account or ciphertext th

- You are not providing the correct symmetric key to the Decrypt API.

Q59)

Your company has 30 years of financial records that take up 15TB of on-premises storage. It is regulated that you maintain these records, but in the year you have worked for the company no one has ever requested any of this data.

Given that the company data center is already filling the bandwidth of its Internet connection, what is an alternative way to store the data on the most appropriate cloud storage?

- AWS Import/Export to Amazon Simple Storage Service (Amazon S3)
- ✅ AWS Import/Export to Amazon Glacier

Explanation:-Because the Internet connection is full, the best solution will be based on using AWS Import/Export to ship the data. The most appropriate storage location for data that must be stored, but is very rarely accessed, is Amazon Glacier.

- Amazon Kinesis
- Amazon Elastic MapReduce (AWS EMR)

Q60)

Your company collects information from the point of sale registers at all of its franchise locations. Each month these processes

collect 200TB of information stored in Amazon Simple Storage Service (Amazon S3). Analytics jobs taking 24 hours are performed to gather knowledge from this data.

Which of the following will allow you to perform these analytics in a cost-effective way?

- Copy the data to a persistent Amazon Elastic MapReduce (Amazon EMR) cluster, and run the MapReduce jobs.
- Create an application that reads the information of the Amazon S3 bucket and runs it through an Amazon Kinesis stream.
- ✅ Run a transient Amazon EMR cluster, and run the MapReduce jobs against the data directly in Amazon S3.

Explanation:-Because the job is run monthly, a persistent cluster will incur unnecessary compute costs during the rest of the month. Amazon Kinesis is not appropriate because the company is running analytics as a batch job and not on a stream. A single large instance does not scale out to accommodate the large compute needs.

- Launch a d2.8xlarge (32 vCPU, 244GB RAM) Amazon Elastic Compute Cloud (Amazon EC2) instance, and run an application to read and process each object sequentially.

Q61) Which service allows you to process nearly limitless streams of data in flight?

- Amazon Kinesis Firehose
- Amazon Elastic MapReduce (Amazon EMR)
- Amazon Redshift
- ✅ Amazon Kinesis Streams

Explanation:-The Amazon Kinesis services enable you to work with large data streams. Within the Amazon Kinesis family of services, Amazon Kinesis Firehose saves streams to AWS storage services, while Amazon Kinesis Streams provide the ability to process the data in the stream.

Q62) What combination of services enable you to copy daily 50TB of data to Amazon storage, process the data in Hadoop, and store the results in a large data warehouse?

- Amazon Kinesis, Amazon Data Pipeline, Amazon Elastic MapReduce (Amazon EMR), and Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Block Store (Amazon EBS), Amazon Data Pipeline, Amazon EMR, and Amazon Redshift
- ✅ Amazon Simple Storage Service (Amazon S3), Amazon Data Pipeline, Amazon EMR, and Amazon Redshift

Explanation:-Amazon Data Pipeline allows you to run regular Extract, Transform, Load (ETL) jobs on Amazon and on-premises data sources. The best storage for large data is Amazon S3, and Amazon Redshift is a large-scale data warehouse service.

- Amazon S3, Amazon Simple Workflow, Amazon EMR, and Amazon DynamoDB

Q63) Your company has 50,000 weather stations around the country that send updates every 2 seconds. What service will enable you to ingest this stream of data and store it to Amazon Simple Storage Service (Amazon S3) for future processing?

- Amazon Simple Queue Service (Amazon SQS)
- ✅ Amazon Kinesis Firehose

Explanation:-Amazon Kinesis Firehose allows you to ingest massive streams of data and store the data on Amazon S3 (as well as Amazon Redshift and Amazon Elasticsearch).

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Data Pipeline

Q64) Your organization uses Chef heavily for its deployment automation. What AWS cloud service provides integration with Chef recipes to start new application server instances, configure application server software, and deploy applications?

- AWS Elastic Beanstalk
- Amazon Kinesis
- ✅ AWS OpsWorks

Explanation:-AWS OpsWorks uses Chef recipes to start new app server instances, configure application server software, and deploy applications. Organizations can leverage Chef recipes to automate operations like software configurations, package installations, database setups, server scaling, and code deployment.

- AWS CloudFormation

Q65)

A firm is moving its testing platform to AWS to provide developers with instant access to clean test and development environments. The primary requirement for the firm is to make environments easily reproducible and fungible.

What service will help the firm meet their requirements?

- ✅ AWS CloudFormation

Explanation:-With AWS CloudFormation, you can reuse your template to set up your resources consistently and repeatedly. Just describe your resources once and then provision the same resources over and over in multiple stacks.

- AWS Config
- Amazon Redshift
- AWS Trusted Advisor

Q66)

Your company's IT management team is looking for an online tool to provide recommendations to save money, improve system availability and performance, and to help close security gaps.

What can help the management team?

- Cloud-init
- ✅ AWS Trusted Advisor

Explanation:-AWS Trusted Advisor inspects your AWS environment and makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps. AWS Trusted Advisor draws upon best practices learned from the aggregated operational history of serving hundreds of thousands of AWS customers.

- AWS Config
- Configuration Recorder

Q67)

Your company works with data that requires frequent audits of your AWS environment to ensure compliance with internal policies and best practices. In order to perform these audits, you need access to historical configurations of your resources to evaluate relevant configuration changes.

Which service will provide the necessary information for your audits?

- ✅ AWS Config

Explanation:-AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing.

- AWS Key Management Service (AWS KMS)
- AWS CloudTrail
- AWS OpsWorks

Q68) All of the website deployments are currently done by your company's development team. With a surge in website popularity, the company is looking for ways to be more agile with deployments. What AWS cloud service can help the developers focus more on writing code instead of spending time managing and configuring servers, databases, load balancers, firewalls, and networks?

- AWS Config
- AWS Trusted Advisor
- Amazon Kinesis
- ✅ AWS Elastic Beanstalk

Explanation:-AWS Elastic Beanstalk is the fastest and simplest way to get an application up and running on AWS. Developers can simply upload their application code, and the service automatically handles all the details such as resource provisioning, load balancing, Auto Scaling, and monitoring.

Q69)

AWS communicates with customers regarding its security and control environment through a variety of different mechanisms.

Which of the following are valid mechanisms? (Choose 3 answers)

- ✅ Obtaining industry certifications and independent third-party attestations

Explanation:-The option describe valid mechanisms that AWS uses to communicate with customers regarding its security and control environment. AWS does not allow customers' auditors direct access to AWS data centers, infrastructure, or staff.

- ✅ Publishing information about security and AWS control practices via the website, whitepapers, and blogs

Explanation:-The option describe valid mechanisms that AWS uses to communicate with customers regarding its security and control environment. AWS does not allow customers' auditors direct access to AWS data centers, infrastructure, or staff.

- ✅ Directly providing customers with certificates, reports, and other documentation (under NDA in some cases)

Explanation:-The option describe valid mechanisms that AWS uses to communicate with customers regarding its security and control environment. AWS does not allow customers' auditors direct access to AWS data centers, infrastructure, or staff.

- Allowing customers' auditors direct access to AWS data centers, infrastructure, and senior staff

---

Q70) Which of the following statements is true when it comes to the AWS shared responsibility model?

- The shared responsibility model is limited to security considerations only; it does not extend to IT controls.
- The shared responsibility model is only applicable for customers who want to be compliant with SOC 1 Type II.
- ✅ The shared responsibility model is not just limited to security considerations; it also extends to IT controls.

Explanation:-The shared responsibility model can include IT controls, and it is not just limited to security considerations. Therefore, answer C is correct.

- The shared responsibility model is only applicable for customers who want to be compliant with ISO 27001.

Q71) AWS provides IT control information to customers in which of the following ways?

- ✅ By using specific control definitions or through general control standard compliance

Explanation:-AWS provides IT control information to customers through either specific control definitions or general control standard compliance.

- By using specific control definitions or through SAS 70
- By using general control standard compliance and by complying with ISO 27001
- By complying with ISO 27001 and SOC 1 Type II

Q72) Which of the following is a valid report, certification, or third-party attestation for AWS? (Choose 3 answers)

- ✅ SOC 1
- ✅ PCI DSS Level 1
- SOC 4

Explanation:-There is no such thing as a SOC 4 report, therefore answer is incorrect.

- ✅ ISO 27001

Q73) Which of the following statements is true?

- ✅ IT governance is still the customer's responsibility, despite deploying their IT estate onto the AWS platform.

Explanation:-IT governance is still the customer's responsibility.

- The AWS platform is PCI DSS-compliant to Level 1. Customers can deploy their web applications to this platform, and they will be PCI DSS-compliant automatically.
- The shared responsibility model applies to IT security only; it does not relate to governance.
- AWS doesn't take risk management very seriously, and it's up to the customer to mitigate risks to the AWS infrastructure.

Q74) Which of the following statements is true when it comes to the risk and compliance advantages of the AWS environment?

- Workloads must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations.
- The critical components of a workload must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations, but the non-critical components do not.
- The non-critical components of a workload must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations, but the critical components do not.
- ✅ Few, many, or all components of a workload can be moved to the AWS Cloud, but it is the customer's responsibility to ensure that their entire workload remains compliant with various certifications and third-party attestations.

Explanation:-Any number of components of a workload can be moved into AWS, but it is the customer's responsibility to ensure that the entire workload remains compliant with various certifications and third-party attestations.

Q75) Which of the following statements best describes an Availability Zone?

- Each Availability Zone consists of a single discrete data center with redundant power and networking/connectivity.
- ✅ Each Availability Zone consists of multiple discrete data centers with redundant power and networking/connectivity.

Explanation:-An Availability Zone consists of multiple discrete data centers, each with their own redundant power and networking/connectivity, therefore answer is correct.

- Each Availability Zone consists of multiple discrete regions, each with a single data center with redundant power and networking/connectivity.
- Each Availability Zone consists of multiple discrete data centers with shared power and redundant networking/connectivity

---

Q76) With regard to vulnerability scans and threat assessments of the AWS platform, which of the following statements are true? (Choose 2 answers)

- ✅ AWS regularly performs scans of public-facing endpoint IP addresses for vulnerabilities.

Explanation:-AWS regularly scans public-facing, non-customer endpoint IP addresses and notifies appropriate parties. AWS does not scan customer instances, and customers must request the ability to perform their own scans in advance, therefore answers are correct.

- Scans performed by AWS include customer instances.
- ✅ AWS security notifies the appropriate parties to remediate any identified vulnerabilities.

Explanation:-AWS regularly scans public-facing, non-customer endpoint IP addresses and notifies appropriate parties. AWS does not scan customer instances, and customers must request the ability to perform their own scans in advance, therefore answers are correct.

- Customers can perform their own scans at any time without advance notice.

Q77) Which of the following best describes the risk and compliance communication responsibilities of customers to AWS?

- AWS and customers both communicate their security and control environment information to each other at all times.
- ✅ AWS publishes information about the AWS security and control practices online, and directly to customers under NDA. Customers do not need to communicate their use and configurations to AWS.

Explanation:-AWS publishes information publicly online and directly to customers under NDA, but customers are not required to share their use and configuration information with AWS, therefore answer is correct.

- Customers communicate their use and configurations to AWS at all times. AWS does not communicate AWS security and control practices to customers for security reasons.
- Both customers and AWS keep their security and control practices entirely confidential and do not share them in order to ensure the greatest security for all parties.

Q78) When it comes to risk management, which of the following is true?

- AWS does not develop a strategic business plan; risk management and mitigation is entirely the responsibility of the customer.
- AWS has developed a strategic business plan to identify any risks and implemented controls to mitigate or manage those risks. Customers do not need to develop and maintain their own risk management plans.
- ✅ AWS has developed a strategic business plan to identify any risks and has implemented controls to mitigate or manage those risks. Customers should also develop and maintain their own risk management plans to ensure they are compliant with any relevant controls and certifications

Explanation:-AWS has developed a strategic business plan, and customers should also develop and maintain their own risk management plans, therefore answer is correct.

- Neither AWS nor the customer needs to worry about risk management, so no plan is needed from either party.

Q79) The AWS control environment is in place for the secure delivery of AWS Cloud service offerings. Which of the following does the collective control environment NOT explicitly include?

- People
- ✅ Energy

Explanation:-The collective control environment includes people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of AWS control framework. Energy is not a discretely identified part of the control environment, therefore this the correct answer.

- Technology
- Processes

Q80) Who is responsible for the configuration of security groups in an AWS environment?

- The customer and AWS are both jointly responsible for ensuring that security groups are correctly and securely configured.
- AWS is responsible for ensuring that all security groups are correctly and securely configured. Customers do not need to worry about security group configuration.
- Neither AWS nor the customer is responsible for the configuration of security groups; security groups are intelligently and automatically configured using traffic heuristics.
- ✅ AWS provides the security group functionality as a service, but the customer is responsible for correctly and securely configuring their own security groups.

Explanation:-Customers are responsible for ensuring all of their security group configurations are appropriate for their own applications, therefore answer is correct.

Q81) Which of the following is NOT a recommended approach for customers trying to achieve strong compliance and governance over an entire IT control environment?

- Take a holistic approach: review information available from AWS together with all other information, and document all compliance requirements.
- Verify that all control objectives are met and all key controls are designed and operating effectively.
- ✅ Implement generic control objectives that are not specifically designed to meet their organization's compliance requirements.

Explanation:-Customers should ensure that they implement control objectives that are designed to meet their organization's own unique compliance requirements, therefore answer is correct.

- Identify and document controls owned by all third parties.

Q82)

You are changing your application to move session state information off the individual Amazon Elastic Compute Cloud (Amazon EC2) instances to take advantage of the elasticity and cost benefits provided by Auto Scaling.

Which of the following AWS Cloud services is best suited as an alternative for storing session state information?

- ✅ Amazon DynamoDB

Explanation:-Amazon DynamoDB is a NoSQL database store that is a great choice as an alternative due to its scalability, high-availability, and durability characteristics. Many platforms provide open-source, drop-in replacement libraries that allow you to store native sessions in Amazon DynamoDB. Amazon DynamoDB is a great candidate for a session storage solution in a share-nothing, distributed architecture.

- Amazon Redshift
- Amazon Storage Gateway
- Amazon Kinesis

Q83)

A media sharing application is producing a very high volume of data in a very short period of time. Your back-end services are unable to manage the large volume of transactions.

What option provides a way to manage the flow of transactions to your back-end services?

- Store the inbound transactions in an Amazon Relational Database Service (Amazon RDS) instance so that your back-end services can retrieve them as time permits.
- ✅ Use an Amazon Simple Queue Service (Amazon SQS) queue to buffer the inbound transactions.

Explanation:-Amazon SQS is a fast, reliable, scalable, and fully managed message queuing service. Amazon SQS should be used to decouple the large volume of inbound transactions, allowing the back-end services to manage the level of throughput without losing messages.

- Use an Amazon Simple Notification Service (Amazon SNS) topic to buffer the inbound transactions.
- Store the inbound transactions in an Amazon Elastic MapReduce (Amazon EMR) cluster so that your back-end services can retrieve them as time permits.

Q84) Which of the following are best practices for managing AWS Identity and Access Management (IAM) user access keys? (Choose 3 answers)

- Embed access keys directly into application code.
- ✅ Use different access keys for different applications.

Explanation:-You should protect AWS user access keys like you would your credit card numbers or any other sensitive secret. Use different access keys for different applications so that you can isolate the permissions and revoke the access keys for individual applications if an access key is exposed. Remember to change access keys on a regular basis. For increased security, it is recommended to configure MFA for any sensitive operations. Remember to remove any IAM users that are no longer needed.

- ✅ Rotate access keys periodically.

Explanation:-You should protect AWS user access keys like you would your credit card numbers or any other sensitive secret. Use different access keys for different applications so that you can isolate the permissions and revoke the access keys for individual applications if an access key is exposed. Remember to change access keys on a regular basis. For increased security, it is recommended to configure MFA for any sensitive operations. Remember to remove any IAM users that are no longer needed.

- Keep unused access keys for an indefinite period of time.
- ✓ Configure Multi-Factor Authentication (MFA) for your most sensitive operations.

Explanation:-You should protect AWS user access keys like you would your credit card numbers or any other sensitive secret. Use different access keys for different applications so that you can isolate the permissions and revoke the access keys for individual applications if an access key is exposed. Remember to change access keys on a regular basis. For increased security, it is recommended to configure MFA for any sensitive operations. Remember to remove any IAM users that are no longer needed.

Q85)

You need to implement a service to scan Application Program Interface (API) calls and related events' history to your AWS account. This service will detect things like unused permissions, overuse of privileged accounts, and anomalous logins.

Which of the following AWS Cloud services can be leveraged to implement this service? (Choose 3 answers)

- ✓ AWS CloudTrail

Explanation:-You can enable AWS CloudTrail in your AWS account to get logs of API calls and related events' history in your account. AWS CloudTrail records all of the API access events as objects in an Amazon S3 bucket that you specify at the time you enable AWS CloudTrail. You can take advantage of Amazon S3's bucket notification feature by directing Amazon S3 to publish object-created events to AWS Lambda. Whenever AWS CloudTrail writes logs to your Amazon S3 bucket, Amazon S3 can then invoke your AWS Lambda.

- ✓ Amazon Simple Storage Service (Amazon S3)

Explanation:-You can enable AWS CloudTrail in your AWS account to get logs of API calls and related events' history in your account. AWS CloudTrail records all of the API access events as objects in an Amazon S3 bucket that you specify at the time you enable AWS CloudTrail. You can take advantage of Amazon S3's bucket notification feature by directing Amazon S3 to publish object-created events to AWS Lambda. Whenever AWS CloudTrail writes logs to your Amazon S3 bucket, Amazon S3 can then invoke your AWS Lambda.

- Amazon Route 53
- Auto Scaling
- ✓ AWS Lambda

Explanation:-You can enable AWS CloudTrail in your AWS account to get logs of API calls and related events' history in your account. AWS CloudTrail records all of the API access events as objects in an Amazon S3 bucket that you specify at the time you enable AWS CloudTrail. You can take advantage of Amazon S3's bucket notification feature by directing Amazon S3 to publish object-created events to AWS Lambda. Whenever AWS CloudTrail writes logs to your Amazon S3 bucket, Amazon S3 can then invoke your AWS Lambda.

Q86)

Government regulations require that your company maintain all correspondence for a period of seven years for compliance reasons.

What is the best storage mechanism to keep this data secure in a cost-effective manner?

- Amazon S3
- ✓ Amazon Glacier

Explanation:-Amazon Glacier enables businesses and organizations to retain data for months, years, or decades, easily and cost effectively. With Amazon Glacier, customers can retain more of their data for future analysis or reference, and they can focus on their business instead of operating and maintaining their storage infrastructure. Customers can also use Amazon Glacier Vault Lock to meet regulatory and compliance archiving requirements.

- Amazon EBS
- Amazon EFS

Q87)

Your company provides media content via the Internet to customers through a paid subscription model. You leverage Amazon CloudFront to distribute content to your customers with low latency.

What approach can you use to serve this private content securely to your paid subscribers?

- ✓ Provide signed Amazon CloudFront URLs to authenticated users to access the paid content.

Explanation:-Many companies that distribute content via the Internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, such as users who have paid a fee. To serve this private content securely using Amazon CloudFront, you can require that users access your private content by using special Amazon CloudFront-signed URLs or signed cookies.

- Use HTTPS requests to ensure that your objects are encrypted when Amazon CloudFront serves them to viewers.
- Configure Amazon CloudFront to compress the media files automatically for paid subscribers.
- Use the Amazon CloudFront geo restriction feature to restrict access to all of the paid subscription media at the country level.

Q88)

Your company provides transcoding services for amateur producers to format their short films to a variety of video formats.

Which service provides the best option for storing the videos?

- Amazon Glacier
- ✓ Amazon Simple Storage Service (Amazon S3)

Explanation:-Amazon S3 provides highly durable and available storage for a variety of content. Amazon S3 can be used as a big data object store for all of the videos. Amazon S3's low cost combined with its design for durability of 99.999999999% and for up to 99.99% availability make it a great storage choice for transcoding services.

- Amazon Relational Database Service (Amazon RDS)
- AWS Storage Gateway

Q89)

A week before Cyber Monday last year, your corporate data center experienced a failed air conditioning unit that caused flooding into the server racks. The resulting outage cost your company significant revenue. Your CIO mandated a move to the cloud, but he is still concerned about catastrophic failures in a data center.

What can you do to alleviate his concerns?

- ✓ Distribute the architecture across multiple Availability Zones.

Explanation:-An Availability Zone consists of one or more physical data centers. Availability zones within a region provide inexpensive, low-latency network connectivity to other zones in the same region. This allows you to distribute your application across data centers. In the event of a catastrophic failure in a data center, the application will continue to handle requests.

- Use an Amazon Virtual Private Cloud (Amazon VPC) with subnets.
- Launch the compute for the processing services in a placement group.
- Purchase Reserved Instances for the processing services instances.
