Answer Sheet

Q1)

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?

● AWS Directory Service and AWS IAM
✓ A VPN connection, and AWS Directory Services
Explanation:-A security principle is a-crum_add_start--->
● A VPN connection, VPC NACLs and Security Groups
● Amazon EC2, and AWS IAM

Q2)

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, 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/
● 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/

Q3)

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 enabled 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 disabled and multi-AZ with automatic failover

---

Q4) 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 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/
● 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/

Q5)

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?

● Deploy NAT Instances in a public subnet
● Create a VPC endpoint
✓ 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/
● Use a NAT Gateway

Q6)

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/

Q7)

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?

✓ 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
● Microsoft SQL Server
● Oracle
● MySQL

Q8) 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?

● Kinesis Firehose
✓ 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/
● RedShift
● EMR

Q9)

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)

✓ 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
● 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

Q10) 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 session affinity (sticky session)
✓ 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 proxy protocol
● ELB Cross zone load balancing

Q11)

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)

✓ 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
● Host the website using AWS Elastic Beanstalk, and map a Route 53 Alias record to the Beanstalk stack
● Host the website on an Amazon EC2 instance, and map a Route 53 Alias record to the public IP address of the EC2 instance
✓ 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

Q12) 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/

Q13) 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)

✓ 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 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/
● Make use of AWS S3 bucket policies to control access to the data at rest

● Use CloudHSM

Q14)

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/

Q15)

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?

● Route 53
✓ 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/

● API Gateway
● IAM Role Based Access Control

Q16) 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?

● Promoting a Read Replica
● Updating DB parameter groups
✓ 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

● Selecting the Multi-AZ feature

Q17)

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?

● Integrate IAM with a user pool in Cognito
✓ 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

● Enable multi-factor authentication (MFA) in IAM
● Integrate a third-party identity provider (IdP)

Q18)

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

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?

● Use CloudFront to cache the content
● Reduce the number of Scan operations
✓ 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/
● 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?

● 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/
● Create a group and add the users to it
● 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 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/

● 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/

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?

● 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

● Elastic Beanstalk

● 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 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

✅ 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 before the Auto Scaling group scales out, the EC2 instances can apply system updates

● 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?

● Elastic Beanstalk

✅ 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/

● Opsworks Stacks

● CloudFormation

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)

● 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/

● Attach an Internet Gateway to the private subnets

✅ 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/

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)

✅ 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/

● AWS Cognito

✅ 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/

● Elastic Load Balancer

Q30) 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 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 an A record pointing to the DNS name of the load balancer

● Create a CNAME record that is an Alias, and select the ELB DNS as a target

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

Q31)

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 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/

● Connect the ELBs using CNAME records

✓ 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/

Q32)

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?

● Provisioned IOPS (IO1)

✓ 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

● Throughput Optimized HDD (ST1)

● Cold HDD (SC1)

Q33) 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)

● 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/

● 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/

Q34) You are a Solutions Architect at Digital Cloud Training. A new client who has not used cloud computing has asked you to explain how AWS works. The client wants to know what service is provided that will provide a virtual network infrastructure that loosely resembles a traditional data center but has the capacity to scale more easily?

● Elastic Compute Cloud

✓ Virtual Private Cloud

Explanation:-Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. It is analogous to having your own DC inside AWS and provides complete control over the virtual networking environment including selection of IP ranges, creation of subnets, and configuration of route tables and gateways. A VPC is logically isolated from other VPCs on AWS Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

● Direct Connect

● Elastic Load Balancing

Q35)

An application you manage in your VPC uses an Auto Scaling Group that spans 3 AZs and there are currently 4 EC2 instances running in the group.

What actions will Auto Scaling take, by default, if it needs to terminate an EC2 instance? (choose 2)

✓ Terminate an instance in the AZ which currently has 2 running EC2 instances

Explanation:-Auto Scaling can perform rebalancing when it finds that the number of instances across AZs is not balanced. Auto Scaling rebalances by launching new EC2 instances in the AZs that have fewer instances first, only then will it start terminating instances in AZs that had more instances Auto Scaling can be configured to send an SNS email when: - An instance is launched - An instance is terminated - An instance fails to launch - An instance fails to terminate Auto Scaling does not terminate the instance that has been running the longest Auto Scaling will only terminate an instance randomly after it has first gone through several other selection steps. Please see the AWS article below for detailed information on the process References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

● Randomly select one of the 3 AZs, and then terminate an instance in that AZ

● Terminate the instance with the least active network connections. If multiple instances meet this criterion, one will be randomly selected

✓ Send an SNS notification, (if configured)

Explanation:-Auto Scaling can perform rebalancing when it finds that the number of instances across AZs is not balanced. Auto Scaling rebalances by launching new EC2 instances in the AZs that have fewer instances first, only then will it start terminating instances in AZs that had more instances Auto Scaling can be configured to send an SNS email when: - An instance is launched - An instance is terminated - An instance fails to launch - An instance fails to terminate Auto Scaling does not terminate the instance that has been running the longest Auto Scaling will only terminate an instance randomly after it has first gone through several other selection steps. Please see the AWS article below for detailed information on the process References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/ https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

Q36)

You're trying to explain to a colleague typical use cases where you can use the Simple Workflow Service (SWF).

Which of the scenarios below would be valid? (choose 2)

● Sending notifications via SMS when an EC2 instance reaches a certain threshold

✓ Managing a multi-step and multi-decision checkout process for a mobile application

Explanation:-Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks You should use Amazon SNS for sending SMS messages You should use CloudFront if you need a CDN Yo should use SQS for storing messages in a queue References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-swf/

● Providing a reliable, highly-scalable, hosted queue for storing messages in transit between EC2 instances

✓ Coordinating business process workflows across distributed application components

Explanation:-Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks You should use Amazon SNS for sending SMS messages You should use CloudFront if you need a CDN Yo should use SQS for storing messages in a queue References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-swf/

Q37)

You work for a systems integrator running a platform that stores medical records. The government security policy mandates that patient data that contains personally identifiable information (PII) must be encrypted at all times, both at rest and in transit.

You are using Amazon S3 to back up data into the AWS cloud.How can you ensure the medical records are properly secured? (choose 2)

● Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-128

✓ Enable Server Side Encryption with S3 managed keys on an S3 bucket using AES-256

Explanation:-When data is stored in an encrypted state it is referred to as encrypted "at rest" and when it is encrypted as it is being transferred over a network it is referred to as encrypted "in transit". You can securely upload/download your data to Amazon S3 via SSL endpoints using the HTTPS protocol (In Transit – SSL/TLS). You have the option of encrypting the data locally before it is uploaded or uploading using SSL/TLS so it is secure in transit and encrypting on the Amazon S3 side using S3 managed keys. The S3 managed keys will be AES-256 (not AES-128) bit keys Uploading data using CloudFront with an EC2 origin or using an encrypted EBS volume attached to an EC2 instance is not a solution to this problem as your company wants to backup these records onto S3 (not EC2/EBS) References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

● Attach an encrypted EBS volume to an EC2 instance

✓ Before uploading the data to S3 over HTTPS, encrypt the data locally using your own encryption keys

Explanation:-When data is stored in an encrypted state it is referred to as encrypted "at rest" and when it is encrypted as it is being transferred over a network it is referred to as encrypted "in transit". You can securely upload/download your data to Amazon S3 via SSL endpoints using the HTTPS protocol (In Transit – SSL/TLS). You have the option of encrypting the data locally before it is uploaded or uploading using SSL/TLS so it is secure in transit and encrypting on the Amazon S3 side using S3 managed keys. The S3 managed keys will be AES-256 (not AES-128) bit keys Uploading data using CloudFront with an EC2 origin or using an encrypted EBS volume attached to an EC2 instance is not a solution to this problem as your company wants to backup these records onto S3 (not EC2/EBS) References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

Q38)

You are a Developer working for Digital Cloud Training. You are planning to write some code that creates a URL that lets users who sign in to your organization's network securely access the AWS Management Console. The URL will include a sign-in token that you get from AWS that authenticates the user to AWS. You are using Microsoft Active Directory Federation Services as your identity provider (IdP) which is compatible with SAML 2.0.

Which of the steps below will you need to include when developing your custom identity broker? (choose 2)

● Delegate access to the IdP through the "Configure Provider" wizard in the IAM console
✓ Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user
Explanation:-The aim of this solution is to create a single sign-on solution that enables users signed in to the organization's Active Directory service to be able to connect to AWS resources. When developing a custom identity broker you use the AWS STS service 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). The steps performed by the custom identity broker to sign users into the AWS management console are: Verify that the user is authenticated by your local identity system Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token Construct a URL for the console that includes the token Give the URL to the user or invoke the URL on the user's behalf You cannot generate a pre-signed URL for this purpose using SDKs, delegate access through the IAM console os directly assume IAM roles 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_providers_enable-console-custom-url.html
● Generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET
✓ Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token
Explanation:-The aim of this solution is to create a single sign-on solution that enables users signed in to the organization's Active Directory service to be able to connect to AWS resources. When developing a custom identity broker you use the AWS STS service 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). The steps performed by the custom identity broker to sign users into the AWS management console are: Verify that the user is authenticated by your local identity system Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token Construct a URL for the console that includes the token Give the URL to the user or invoke the URL on the user's behalf You cannot generate a pre-signed URL for this purpose using SDKs, delegate access through the IAM console os directly assume IAM roles 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_providers_enable-console-custom-url.html

Q39)

You have been asked to come up with a solution for providing single sign-on to existing staff in your company who manage on-premise web applications and now need access to the AWS management console to manage resources in the AWS cloud.

Which product combinations provide the best solution to achieve this requirement?

● Use IAM and Amazon Cognito
✓ Use the AWS Secure Token Service (STS) and SAML
Explanation:-Single sign-on using federation allows users to login to the AWS console without assigning IAM credentials 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 (such as federated users from an on-premise directory) Federation (typically Active Directory) uses SAML 2.0 for authentication and grants temporary access based on the users AD credentials. The user does not need to be a user in IAM You cannot use your on-premise LDAP directory with IAM, you must use federation Enabling multi-factor authentication (MFA) for IAM is not a federation solution Amazon Cognito is used for authenticating users to web and mobile apps not for providing single sign-on between on-premises directories and the AWS management console References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/
● Use your on-premise LDAP directory with IAM
● Use IAM and MFA

Q40)

You are putting together the design for a new retail website for a high-profile company. The company has previously been the victim of targeted distributed denial-of-service (DDoS) attacks and have requested that you ensure the design includes mitigation techniques.

Which of the following are the BEST techniques to help ensure the availability of the services is not compromized in an attack? (choose 2)

● Use encryption on your EBS volumes
✓ CloudFront for distributing both static and dynamic content
Explanation:-CloudFront distributes traffic across multiple edge locations and filters requests to ensure that only valid HTTP(S) requests will be forwarded to backend hosts. CloudFront also supports geoblocking, which you can use to prevent requests from particular geographic locations from being served ELB automatically distributes incoming application traffic across multiple targets, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, containers, and IP addresses, and multiple Availability Zones, which minimizes the risk of overloading a single resource ELB, like CloudFront, only supports valid TCP requests, so DDoS attacks such as UDP and SYN floods are not able to reach EC2 instances ELB also offers a single point of management and can serve as a line of defense between the internet and your backend, private EC2 instances Auto Scaling helps to maintain a desired count of EC2 instances running at all times and setting a high maximum number of instances allows your fleet to grow and absorb some of the impact of the attack RDS supports several scenarios for deploying DB instances in private and public facing configurations CloudWatch can be used to setup alerts for when metrics reach unusual levels. High network in traffic may indicate a DDoS attack Encrypting EBS volumes does not help in a DDoS attack as the attack is targeted at reducing availability rather than compromising data Spot instances may reduce the cost (depending on the current Spot price) however the questions asks us to focus on availability not cost References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/ https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/ https://docs.aws.amazon.com/waf/latest/developerguide/tutorials-ddos-cross-service.html https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html
✓ Configure Auto Scaling with a high maximum number of instances to ensure it can scale accordingly
Explanation:-CloudFront distributes traffic across multiple edge locations and filters requests to ensure that only valid HTTP(S) requests will be

forwarded to backend hosts. CloudFront also supports geoblocking, which you can use to prevent requests from particular geographic locations from being served ELB automatically distributes incoming application traffic across multiple targets, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, containers, and IP addresses, and multiple Availability Zones, which minimizes the risk of overloading a single resource ELB, like CloudFront, only supports valid TCP requests, so DDoS attacks such as UDP and SYN floods are not able to reach EC2 instances ELB also offers a single point of management and can serve as a line of defense between the internet and your backend, private EC2 instances Auto Scaling helps to maintain a desired count of EC2 instances running at all times and setting a high maximum number of instances allows your fleet to grow and absorb some of the impact of the attack RDS supports several scenarios for deploying DB instances in private and public facing configurations CloudWatch can be used to setup alerts for when metrics reach unusual levels. High network in traffic may indicate a DDoS attack Encrypting EBS volumes does not help in a DDoS attack as the attack is targeted at reducing availability rather than compromising data Spot instances may reduce the cost (depending on the current Spot price) however the questions asks us to focus on availability not cost References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/ https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/ https://docs.aws.amazon.com/waf/latest/developerguide/tutorials-ddos-cross-service.html https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html

● Use Spot instances to reduce the cost impact in case of attack

---

Q41)

You are creating a series of environments within a single VPC. You need to implement a system of categorization that allows for identification of EC2 resources by business unit, owner, or environment.

Which AWS feature allows you to do this?

● Metadata

✓ Tags

Explanation:-A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment Instance metadata is data about your instance that you can use to configure or manage the running instance Parameters and custom filters are not used for categorization References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

● Parameters

● Custom filters

Q42) You regularly launch EC2 instances manually from the console and want to streamline the process to reduce administrative overhead. What feature of EC2 allows you to store settings such as AMI ID, instance type, key pairs and Security Groups?

● Run Command

● Placement Groups

● Launch Configurations

✓ Launch Templates

Explanation:-Launch templates enable you to store launch parameters so that you do not have to specify them every time you launch an instance. When you launch an instance using the Amazon EC2 console, an AWS SDK, or a command line tool, you can specify the launch template to use Launch Configurations are used with Auto Scaling Groups Run Command automates common administrative tasks, and lets you perform ad hoc configuration changes at scale You can launch or start instances in a placement group, which determines how instances are placed on underlying hardware References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-templates.html

---

Q43)

You are a Solutions Architect for a pharmaceutical company. The company uses a strict process for release automation that involves building and testing services in 3 separate VPCs. A peering topology is configured with VPC-A peered with VPC-B and VPC-B peered with VPC-C. The development team wants to modify the process so that they can release code directly from VPC-A to VPC-C.

How can this be accomplished?

● Update VPC-Bs route table with peering targets for VPC-A and VPC-C and enable route propagation

● Update the CIDR blocks to match to enable inter-VPC routing

● Update VPC-As route table with an entry using the VPC peering as a target

✓ Create a new VPC peering connection between VPC-A and VPC-C

Explanation:-It is not possible to use transitive peering relationships with VPC peering and therefore you must create an additional VPC peering connection between VPC-A and VPC-C You must update route tables to configure routing however updating VPC-As route table alone will not lead to the desired result without first creating the additional peering connection Route propagation cannot be used to extend VPC peering connections You cannot have matching (overlapping) CIDR blocks with VPC peering References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q44)

You are a Solutions Architect for Digital Cloud Training. A client is migrating a large amount of data that their customers access onto the AWS cloud. The client is located in Australia and most of their customers will be accessing the data from within Australia. The customer has asked you for some advice about S3 buckets.

Which of the following statements would be good advice? (choose 2)

✓ To reduce latency and improve performance, create the buckets in the Asia Pacific (Sydney) region

Explanation:-For better performance, lower latency and lower costs the buckets should be created in the region that is closest to the client's customers S3 is a universal namespace so names must be unique globally Bucket names cannot be changed after they have been created An S3 bucket is created within a region and all replicated copies of the data stay within the region unless you explicitly configure cross-region replication There is no limit on the number of objects you can store in an S3 bucket References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

● S3 is a global service so it doesn’t matter where you create your buckets
● Buckets can be renamed after they have been created
✓ S3 is a universal namespace so bucket names must be unique globally
Explanation:-For better performance, lower latency and lower costs the buckets should be created in the region that is closest to the client's customers S3 is a universal namespace so names must be unique globally Bucket names cannot be changed after they have been created An S3 bucket is created within a region and all replicated copies of the data stay within the region unless you explicitly configure cross-region replication There is no limit on the number of objects you can store in an S3 bucket References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

Q45)

There is a problem with an EC2 instance that was launched by AWS Auto Scaling. The EC2 status checks have reported that the instance is “Impaired??.

What action will AWS Auto Scaling take?

● Auto Scaling performs its own status checks and does not integrate with EC2 status checks
✓ It will mark the instance for termination, terminate it, and then launch a replacement
Explanation:-If any health check returns an unhealthy status the instance will be terminated. Unlike AZ rebalancing, termination of unhealthy instances happens first, then Auto Scaling attempts to launch new instances to replace terminated instances AS will not launch a new instance immediately as it always terminates unhealthy instance before launching a replacement Auto Scaling does not wait for 300 seconds, once the health check has failed the configured number of times the instance will be terminated Auto Scaling does integrate with EC2 status checks as well as having its own status checks References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/
● It will launch a new instance immediately and then mark the impaired one for replacement
● Auto Scaling will wait for 300 seconds to give the instance a chance to recover

---

Q46)

An Auto Scaling Group is unable to respond quickly enough to load changes resulting in lost messages from another application tier. The messages are typically around 128KB in size.

What is the best design option to prevent the messages from being lost?

● Store the messages on Amazon S3
● Launch an Elastic Load Balancer
✓ Store the messages on an SQS queue
Explanation:-In this circumstance the ASG cannot launch EC2 instances fast enough. You need to be able to store the messages somewhere so they don't get lost whilst the EC2 instances are launched. This is a classic use case for decoupling and SQS is designed for exactly this purpose 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. An SQS queue can be used to create distributed/decoupled applications Storing the messages on S3 is potentially feasible but SQS is the preferred solution as it is designed for decoupling. If the messages are over 256KB and therefore cannot be stored in SQS, you may want to consider using S3 and it can be used in combination with SQS by using the Amazon SQS Extended Client Library for Java An ELB can help to distribute incoming connections to the back-end EC2 instances however if the ASG is not scaling fast enough then there aren't enough resources for the ELB to distributed traffic to References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/
● Use larger EC2 instance sizes

Q47) An application you run on AWS uses an ELB to distribute connections between EC2 instances. You need to record information on the requester, IP, and request type for connections made to the ELB. You will also need to perform some analysis on the log files, which AWS services and configuration options can be used to collect and then analyze the logs? (choose 2)

✓ Enable Access Logs on the ELB and store the log files on S3
Explanation:-The best way to deliver these requirements is to enable access logs on the ELB and then use EMR for analyzing the log files Access Logs on ELB are disabled by default. Information includes information about the clients (not included in CloudWatch metrics) such as the identity of the requester, IP, request type etc. Logs can be optionally stored and retained in S3 Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3 The information recorded by ELB access logs is exactly what you require so there is no need to get the application to record the information into DynamoDB Elastic Transcoder is used for converting media file formats not analyzing files References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/
● Update the application to use DynamoDB for storing log files
● Enable Access Logs on the EC2 instances and store the log files on S3
✓ Use EMR for analyzing the log files
Explanation:-The best way to deliver these requirements is to enable access logs on the ELB and then use EMR for analyzing the log files Access Logs on ELB are disabled by default. Information includes information about the clients (not included in CloudWatch metrics) such as the identity of the requester, IP, request type etc. Logs can be optionally stored and retained in S3 Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3 The information recorded by ELB access logs is exactly what you require so there is no need to get the application to record the information into DynamoDB Elastic Transcoder is used for converting media file formats not analyzing files References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-emr/

Q48)

An EC2 instance in an Auto Scaling Group is having some issues that are causing the ASG to launch new instances based on the dynamic scaling policy. You need to troubleshoot the EC2 instance and prevent the ASG from launching new instances temporarily.

What is the best method to accomplish this? (choose 2)

✓ Suspend the scaling processes responsible for launching new instances

Explanation:-You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. This can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes. You can manually move an instance from an ASG and put it in the standby state Instances in standby state are still managed by Auto Scaling, are charged as normal, and do not count towards available EC2 instance for workload/application use. Auto scaling does not perform health checks on instances in the standby state. Standby state can be used for performing updates/changes/troubleshooting etc. without health checks being performed or replacement instances being launched You do not need to disable the dynamic scaling policy, you can just suspend it as previously described You cannot disable the launch configuration and you can't modify a launch configuration after you've created it Target Groups are features of ELB (specifically ALB/NLB). Removing the instance from the target group will stop the ELB from sending connections to it but will not stop Auto Scaling from launching new instances while you are troubleshooting it References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

● Remove the EC2 instance from the Target Group

✓ Place the EC2 instance that is experiencing issues into the Standby state

Explanation:-You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. This can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes. You can manually move an instance from an ASG and put it in the standby state Instances in standby state are still managed by Auto Scaling, are charged as normal, and do not count towards available EC2 instance for workload/application use. Auto scaling does not perform health checks on instances in the standby state. Standby state can be used for performing updates/changes/troubleshooting etc. without health checks being performed or replacement instances being launched You do not need to disable the dynamic scaling policy, you can just suspend it as previously described You cannot disable the launch configuration and you can't modify a launch configuration after you've created it Target Groups are features of ELB (specifically ALB/NLB). Removing the instance from the target group will stop the ELB from sending connections to it but will not stop Auto Scaling from launching new instances while you are troubleshooting it References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

● Disable the dynamic scaling policy

Q49)

An important application you manage uses an Elastic Load Balancer (ELB) to distribute incoming requests amongst a fleet of EC2 instances. You need to ensure any operational issues are identified.

Which of the statements below are correct about monitoring of an ELB? (choose 2)

● CloudWatch metrics can be logged to an S3 bucket

✓ Information is sent to CloudWatch every minute if there are active requests

Explanation:-Information is sent by the ELB to CloudWatch every 1 minute when requests are active. Can be used to trigger SNS notifications Access Logs are disabled by default. Includes information about the clients (not included in CloudWatch metrics) including identifying the requester, IP, request type etc. Access logs can be optionally stored and retained in S3 CloudWatch metrics for ELB cannot be logged directly to an S3 bucket. Instead you should use ELB access logs CloudTrail is used to capture API calls to the ELB and logs can be stored in an S3 bucket References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

✓ Access logs can identify requester, IP, and request type

Explanation:-Information is sent by the ELB to CloudWatch every 1 minute when requests are active. Can be used to trigger SNS notifications Access Logs are disabled by default. Includes information about the clients (not included in CloudWatch metrics) including identifying the requester, IP, request type etc. Access logs can be optionally stored and retained in S3 CloudWatch metrics for ELB cannot be logged directly to an S3 bucket. Instead you should use ELB access logs CloudTrail is used to capture API calls to the ELB and logs can be stored in an S3 bucket References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

● Access logs are enabled by default

Q50) An application that you manage uses a combination of Reserved and On-Demand instances to handle typical load. The application involves performing analytics on a set of data and you need to temporarily deploy a large number of EC2 instances. You only need these instances to be available for a short period of time until the analytics job is completedIf job completion is not time-critical what is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

● Use Reserved instances

● Use dedicated hosts

✓ Use Spot instances

Explanation:-The key requirements here are that you need to temporarily deploy a large number of instances, can tolerate an delay (not time-critical), and need the most economical solution. In this case Spot instances are likely to be the most economical solution. You must be able to tolerate delays if using Spot instances as if the market price increases your instances will be terminated and you may have to wait for the price to lower back to your budgeted allowance. On-demand is good for temporary deployments when you cannot tolerate any delays (instances being terminated by AWS). It is likely to be more expensive than Spot however so if delays can be tolerated it is not the best solution Reserved instances are used for longer more stable requirements where you can get a discount for a fixed 1 or 3 year term. This pricing model is not good for temporary requirements An EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. They are much more expensive than on-demand or Spot instances and are used for use cases such as bringing your own socket-based software licences to AWS or for compliance reasons References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

● Use On-Demand instances