Answer Sheet

Q1) You have just initiated the creation of a snapshot of an EBS volume and the snapshot process is currently in operation. Which of the statements below is true regarding the operations that are possible while the snapshot process in running?

- The volume can be used in read-only mode while the snapshot is in progress
- The volume cannot be used until the snapshot completes
- The volume can be used in write-only mode while the snapshot is in progress
- ✅ The volume can be used as normal while the snapshot is in progress

Explanation:-You can take a snapshot of an EBS volume while the instance is running and it does not cause any outage of the volume so it can continue to be used as normal. However, the advice is that to take consistent snapshots writes to the volume should be stopped. For non-root EBS volumes this can entail taking the volume offline (detaching the volume with the instance still running), and for root EBS volumes it entails shutting down the instance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html

---

Q2)

A Solutions Architect is creating a solution for an application that must be deployed on Amazon EC2 hosts that are dedicated to the client. Instance placement must be automatic and billing should be per instance.

Which type of EC2 deployment model should be used?

- Reserved Instance
- ✅ Dedicated Instance

Explanation:-Dedicated Instances are Amazon EC2 instances that run in a VPC on hardware that's dedicated to a single customer. Your Dedicated instances are physically isolated at the host hardware level from instances that belong to other AWS accounts. Dedicated instances allow automatic instance placement and billing is per instance An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts can help you address compliance requirements and reduce costs by allowing you to use your existing server-bound software licenses. With dedicated hosts billing is on a per-host basis (not per instance) Reserved instances are a method of reducing cost by committing to a fixed contract term of 1 or 3 years A Cluster Placement Group determines how instances are placed on underlying hardware to enable low-latency connectivity References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://aws.amazon.com/ec2/dedicated-hosts/

- Dedicated Host
- Cluster Placement Group

Q3)

A Solutions Architect is designing the compute layer of a serverless application. The compute layer will manage requests from external systems, orchestrate serverless workflows, and execute the business logic.The Architect needs to select the most appropriate AWS services for these functions.

Which services should be used for the compute layer? (choose 2)

- ✅ Use Amazon API Gateway with AWS Lambda for executing the business logic

Explanation:-With Amazon API Gateway, you can run a fully managed REST API that integrates with Lambda to execute your business logic and includes traffic management, authorization and access control, monitoring, and API versioning AWS Step Functions orchestrates serverless workflows including coordination, state, and function chaining as well as combining long-running executions not supported within Lambda execution limits by breaking into multiple steps or by calling workers running on Amazon Elastic Compute Cloud (Amazon EC2) instances or on-premises The Amazon Elastic Container Service (ECS) is not a serverless application stack, containers run on EC2 instances AWS CloudFormation and Elastic Beanstalk are orchestrators that are used for describing and provisioning resources not actually performing workflow functions within the application References: https://aws.amazon.com/step-functions/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

- Use AWS Elastic Beanstalk for executing the business logic
- ✅ Use AWS Step Functions for orchestrating serverless workflows

Explanation:-With Amazon API Gateway, you can run a fully managed REST API that integrates with Lambda to execute your business logic and includes traffic management, authorization and access control, monitoring, and API versioning AWS Step Functions orchestrates serverless workflows including coordination, state, and function chaining as well as combining long-running executions not supported within Lambda execution limits by breaking into multiple steps or by calling workers running on Amazon Elastic Compute Cloud (Amazon EC2) instances or on-premises The Amazon Elastic Container Service (ECS) is not a serverless application stack, containers run on EC2 instances AWS CloudFormation and Elastic Beanstalk are orchestrators that are used for describing and provisioning resources not actually performing workflow functions within the application References: https://aws.amazon.com/step-functions/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

- Use Amazon ECS for executing the business logic

Q4)

You are a Solutions Architect for Digital Cloud Training. A client has asked for some assistance in selecting the best database for a specific requirement. The database will be used for a data warehouse solution and the data will be stored in a structured format. The client wants to run complex analytics queries using business intelligence tools.

Which AWS database service will you recommend?

- ✅ RedShift

Explanation:-Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools. RedShift is a SQL based data warehouse used for analytics applications. RedShift is an Online Analytics Processing (OLAP) type of DB. RedShift is used for running complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution Amazon RDS does store data in a structured format but it is not a data warehouse. The primary use case for RDS is as a transactional database (not an analytics database) Amazon DynamoDB is not a structured database (schema-less / NoSQL) and is not a data warehouse solution Amazon Aurora is a type of RDS

database so is also not suitable for a data warehouse use case References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

- Aurora
- RDS
- DynamoDB

Q5) You would like to provide some elasticity for your RDS DB. You are considering read replicas and are evaluating the features. Which of the following statements are applicable when using RDS read replicas? (choose 2)

- ✅ It is possible to have read-replicas of read-replicas

Explanation:-Multi-AZ utilizes failover and DNS endpoint updates, not read replicas Read replicas are used for read heavy DBs and replication is asynchronous You can have read replicas of read replicas for MySQL and MariaDB but not for PostgreSQL You cannot have more than four instances involved in a replication chain You can specify the AZ the read replica is deployed in References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- ✅ You cannot have more than four instances involved in a replication chain

Explanation:-Multi-AZ utilizes failover and DNS endpoint updates, not read replicas Read replicas are used for read heavy DBs and replication is asynchronous You can have read replicas of read replicas for MySQL and MariaDB but not for PostgreSQL You cannot have more than four instances involved in a replication chain You can specify the AZ the read replica is deployed in References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- You cannot specify the AZ the read replica is deployed in
- Replication is synchronous

Q6)

An application running in your on-premise data center writes data to a MySQL database. You are re-architecting the application and plan to move the database layer into the AWS cloud on RDS. You plan to keep the application running in your on-premise data center.

What do you need to do to connect the application to the RDS database via the Internet? (choose 2)

- Create a DB subnet group that is publicly accessible
- ✅ Choose to make the RDS instance publicly accessible and place it in a public subnet

Explanation:-When you create the RDS instance, you need to select the option to make it publicly accessible. A security group will need to be created and assigned to the RDS instance to allow access from the public IP address of your application (or firewall) NAT Gateways are used for enabling Internet connectivity for EC2 instances in private subnets A DB subnet group is a collection of subnets (typically private) that you create in a VPC and that you then designate for your DB instance. The DB subnet group cannot be made publicly accessible, even if the subnets are public subnets, it is the RDS DB that must be configured to be publicly accessible References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html#USER_VPC.Scenario4

- Configure an NAT Gateway and attach the RDS database
- ✅ Create a security group allowing access from your public IP to the RDS instance and assign to the RDS instance

Explanation:-When you create the RDS instance, you need to select the option to make it publicly accessible. A security group will need to be created and assigned to the RDS instance to allow access from the public IP address of your application (or firewall) NAT Gateways are used for enabling Internet connectivity for EC2 instances in private subnets A DB subnet group is a collection of subnets (typically private) that you create in a VPC and that you then designate for your DB instance. The DB subnet group cannot be made publicly accessible, even if the subnets are public subnets, it is the RDS DB that must be configured to be publicly accessible References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html#USER_VPC.Scenario4

Q7) A Solutions Architect is designing an application stack that will be highly elastic. Which AWS services can be used that don't require you to make any capacity decisions upfront? (choose 2)

- ✅ Amazon Kinesis Firehose

Explanation:-With Kinesis Data Firehose, you only pay for the amount of data you transmit through the service, and if applicable, for data format conversion. There is no minimum fee or setup cost AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running With Amazon EC2 you need to select your instance sizes and number of instances With RDS you need to select the instance size for the DB With DynamoDB you need to specify the read/write capacity of the DB References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

- Amazon EC2
- DynamoDB
- ✅ AWS Lambda

Explanation:-With Kinesis Data Firehose, you only pay for the amount of data you transmit through the service, and if applicable, for data format conversion. There is no minimum fee or setup cost AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running With Amazon EC2 you need to select your instance sizes and number of instances With RDS you need to select the instance size for the DB With DynamoDB you need to specify the read/write capacity of the DB References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

Q8)

An application you manage regularly uploads files from an EC2 instance to S3. The files can be a couple of GB in size and sometimes the uploads are slower than you would like resulting in poor upload times.

What method can be used to increase throughput and speed things up?

- Turn off versioning on the destination bucket
- Upload the files using the S3 Copy SDK or REST API
- Randomize the object names when uploading

✅ Use Amazon S3 multipart upload

Explanation:-Multipart upload can be used to speed up uploads to S3. Multipart upload uploads objects in parts independently, in parallel and in any order. It is performed using the S3 Multipart upload API and is recommended for objects of 100MB or larger. It can be used for objects from 5MB up to 5TB and must be used for objects larger than 5GB Randomizing object names provides no value in this context, random prefixes are used for intensive read requests Copy is used for copying, moving and renaming objects within S3 not for uploading to S3 Turning off versioning will not speed up the upload References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

Q9)

A new department will begin using AWS services in your account and you need to create an authentication and authorization strategy.

Select the correct statements regarding IAM groups? (choose 2)

✅ IAM groups can be used to assign permissions to users

Explanation:-Groups are collections of users and have policies attached to them A group is not an identity and cannot be identified as a principal in an IAM policy Use groups to assign permissions to users IAM groups cannot be used to group EC2 instances Only users and services can assume a role to take on permissions (not groups) References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

⚪ IAM groups can be used to group EC2 instances

⚪ IAM groups can be nested up to 4 levels

✅ An IAM group is not an identity and cannot be identified as a principal in an IAM policy

Explanation:-Groups are collections of users and have policies attached to them A group is not an identity and cannot be identified as a principal in an IAM policy Use groups to assign permissions to users IAM groups cannot be used to group EC2 instances Only users and services can assume a role to take on permissions (not groups) References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

Q10)

You are a Solutions Architect at Digital Cloud Training. In your VPC you have a mixture of EC2 instances in production and non-production environments. You need to devise a way to segregate access permissions to different sets of users for instances in different environments.

How can this be achieved? (choose 2)

⚪ Attach an Identity Provider (IdP) and delegate access to the instances to the relevant groups

⚪ Add an environment variable to the instances using user data

✅ Create an IAM policy that grants access to any instances with the specific tag

Explanation:-You can use the condition checking in IAM policies to look for a specific tag. IAM checks that the tag attached to the principal making the request matches the specified key name and value You cannot achieve this outcome using environment variables stored in user data and conditional statements in a policy. You must use an IAM policy that grants access to instances based on the tag You cannot use an IdP for this solution References: https://aws.amazon.com/premiumsupport/knowledge-center/iam-ec2-resource-tags/ https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

✅ Add a specific tag to the instances you want to grant the users or groups access to

Explanation:-You can use the condition checking in IAM policies to look for a specific tag. IAM checks that the tag attached to the principal making the request matches the specified key name and value You cannot achieve this outcome using environment variables stored in user data and conditional statements in a policy. You must use an IAM policy that grants access to instances based on the tag You cannot use an IdP for this solution References: https://aws.amazon.com/premiumsupport/knowledge-center/iam-ec2-resource-tags/ https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

---

Q11)

The application development team in your company have created a new application written in .NET. You are looking for a way to easily deploy the application whilst maintaining full control of the underlying resources.

Which PaaS service provided by AWS would suit this requirement?

⚪ EC2 Placement Groups

✅ Elastic Beanstalk

Explanation:-AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. It is considered to be a Platform as a Service (PaaS) solution and allows full control of the underlying resources CloudFront is a content delivery network for caching content to improve performance CloudFormation uses templates to provision infrastructure EC2 Placement Groups are used to control how instances are launched to enable low-latency connectivity or to be spread across distinct hardware References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/

⚪ CloudFormation

⚪ CloudFront

Q12)

There is new requirement for a database that will store a large number of records for an online store. You are evaluating the use of DynamoDB.

Which of the following are AWS best practices for DynamoDB? (choose 2)

⚪ Use large files

✅ Store objects larger than 400KB in S3 and use pointers in DynamoDB

Explanation:-DynamoDB best practices include: Keep item sizes small If you are storing serial data in DynamoDB that will require actions based on data/time use separate tables for days, weeks, months Store more frequently and less frequently accessed data in separate tables If possible compress larger attribute values Store objects larger than 400KB in S3 and use pointers (S3 Object ID) in DynamoDB References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

- Use for BLOB data use cases
- ✅ Store more frequently and less frequently accessed data in separate tables

Explanation:-DynamoDB best practices include: Keep item sizes small If you are storing serial data in DynamoDB that will require actions based on data/time use separate tables for days, weeks, months Store more frequently and less frequently accessed data in separate tables If possible compress larger attribute values Store objects larger than 400KB in S3 and use pointers (S3 Object ID) in DynamoDB References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

Q13)

A new application that you rolled out recently runs on Amazon EC2 instances and uses API Gateway and Lambda. Your company is planning on running an advertising campaign that will likely result in significant hits to the application after each ad is run.You're concerned about the impact this may have on your application and would like to put in place some controls to limit the number of requests per second that hit the application.

What controls will you implement in this situation?

- API Gateway and Lambda scale automatically to handle any load so there's no need to implement controls
- ✅ Implement throttling rules on the API Gateway

Explanation:-The key requirement is that you need to limit the number of requests per second that hit the application. This can only be done by implementing throttling rules on the API Gateway. Throttling enables you to throttle the number of requests to your API which in turn means less traffic will be forwarded to your application server Caching can improve performance but does not limit the amount of requests coming in API Gateway and Lambda both scale up to their default limits however the bottleneck is with the application server running on EC2 which may not be able to scale to keep up with demand Lambda continuous scaling does not resolve the scalability concerns with the EC2 application server References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/ https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html

- Enable caching on the API Gateway and specify a size in gigabytes
- Enable Lambda continuous scaling

Q14) You are using encryption with several AWS services and are looking for a solution for secure storage of the keys. Which AWS service provides a hardware-based storage solution for cryptographic keys?

- ✅ CloudHSM

Explanation:-AWS CloudHSM is a cloud-based hardware security module (HSM) that allows you to easily add secure key storage and high-performance crypto operations to your AWS applications CloudHSM is a managed service that automates time-consuming administrative tasks, such as hardware provisioning, software patching, high availability, and backups CloudHSM is one of several AWS services, including AWS Key Management Service (KMS), which offer a high level of security for your cryptographic keys KMS provides an easy, cost-effective way to manage encryption keys on AWS that meets the security needs for the majority of customer data A VPC is a logical networking construct within an AWS account PKI is a term used to describe the whole infrastructure responsible for the usage of public key cryptography References: https://aws.amazon.com/cloudhsm/details/

- Public Key Infrastructure (PKI)
- Virtual Private Cloud (VPC)
- Key Management Service (KMS)

Q15)

You are developing a multi-tier application that includes loosely-coupled, distributed application components and need to determine a method of sending notifications instantaneously.

Using SNS which transport protocols are supported? (choose 2)

- ✅ Email-JSON

Explanation:-Note that the questions asks you which transport protocols are supported, NOT which subscribers - therefore Lambda is not supported SNS supports notifications over multiple transport protocols: HTTP/HTTPS – subscribers specify a URL as part of the subscription registration Email/Email-JSON – messages are sent to registered addresses as email (text-based or JSON-object) SQS – users can specify an SQS standard queue as the endpoint SMS – messages are sent to registered phone numbers as SMS text messages References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/

- SWF
- ✅ HTTPS

Explanation:-Note that the questions asks you which transport protocols are supported, NOT which subscribers - therefore Lambda is not supported SNS supports notifications over multiple transport protocols: HTTP/HTTPS – subscribers specify a URL as part of the subscription registration Email/Email-JSON – messages are sent to registered addresses as email (text-based or JSON-object) SQS – users can specify an SQS standard queue as the endpoint SMS – messages are sent to registered phone numbers as SMS text messages References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/

- Lambda

Q16)

You have deployed a number of AWS resources using CloudFormation. You need to make some changes to a couple of resources within the stack and are planning how to implement the updates. Due to recent bad experiences, you're a little concerned about what the effects of implementing updates to the resources might have on other resources in the stack.

What is the easiest way to proceed cautiously?

- Use a direct update
- ✅ Create and execute a change set

Explanation:-AWS CloudFormation provides two methods for updating stacks: direct update or creating and executing change sets. When you directly update a stack, you submit changes and AWS CloudFormation immediately deploys them. Use direct updates when you want to quickly deploy your updates. With change sets, you can preview the changes AWS CloudFormation will make to your stack, and then decide whether to apply those changes Direct updates will not provide the safeguard of being able to preview the changes as changes sets do You do not need to go

to the trouble and cost of deploying a new stack You cannot use OpsWorks to manage the configuration changes. OpsWorks is used for implementing managed Chef and Puppet services References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/ https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks.html

- Deploy a new stack to test the changes
- Use OpsWorks to manage the configuration changes

Q17)

AWS Regions provide multiple, physically separated and isolated _____ which are connected with low latency, high throughput, and highly redundant networking.

Select the missing term from the options below.

- Subnets
- Edge locations
- Facilities
- ✅ Availability zones

Explanation:-Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones and are connected with low latency, high throughput, and highly redundant networking Subnets are created within availability zones (AZs). Each subnet must reside entirely within one Availability Zone and cannot span zones Each AZ is located in one or more data centers (facilities) An Edge Location is a CDN endpoint for CloudFront References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

---

Q18)

You are a Solutions Architect at Digital Cloud Training. One of your customers runs an application on-premise that stores large media files. The data is mounted to different servers using either the SMB or NFS protocols. The customer is having issues with scaling the storage infrastructure on-premise and is looking for a way to offload the data set into the cloud whilst retaining a local cache for frequently accessed content.

Which of the following is the best solution?

- Use the AWS Storage Gateway Volume Gateway in cached volume mode
- Create a script that migrates infrequently used data to S3 using multi-part upload
- ✅ Use the AWS Storage Gateway File Gateway

Explanation:-File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2-resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching The AWS Storage Gateway Volume Gateway in cached volume mode is a block-based (not file-based) solution so you cannot mount the storage with the SMB or NFS protocols With Cached Volume mode – the entire dataset is stored on S3 and a cache of the most frequently accessed data is cached on-site You could mount EFS over a VPN but it would not provide you a local cache of the data Creating a script the migrates infrequently used data to S3 is possible but that data would then not be indexed on the primary filesystem so you wouldn't have a method of retrieving it without developing some code to pull it back from S3. This is not the best solution References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/

- Establish a VPN and use the Elastic File System (EFS)

Q19) Your operations team would like to be notified if an RDS database exceeds certain metric thresholds. They have asked you how this could be automated?

- Setup an RDS alarm and associate an SNS topic with it that sends an email
- Create a CloudTrail alarm and configure a notification event to send an SMS
- ✅ Create a CloudWatch alarm and associate an SNS topic with it that sends an email notification

Explanation:-You can create a CloudWatch alarm that watches a single CloudWatch metric or the result of a math expression based on CloudWatch metrics. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. The action can be an Amazon EC2 action, an Amazon EC2 Auto Scaling action, or a notification sent to an Amazon SNS topic. SNS can be configured to send an email notification CloudTrail is used for auditing API access, not for performance monitoring CloudWatch performs performance monitoring so you don't setup alarms in RDS itself You cannot associate an SQS queue with a CloudWatch alarm References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/

- Create a CloudWatch alarm and associate an SQS with it that delivers a message to SES

Q20) A Solutions Architect is conducting an audit and needs to query several properties of EC2 instances in a VPC. What two methods are available for accessing and querying the properties of an EC2 instance such as instance ID, public keys and network interfaces? (choose 2)

- Run the command “curl http://169.254.169.254/latest/dynamic/instance-identity/"
- ✅ Run the command “curl http://169.254.169.254/latest/meta-data/"

Explanation:-This information is stored in the instance metadata on the instance. You can access the instance metadata through a URI or by using the Instance Metadata Query tool The instance metadata is available at http://169.254.169.254/latest/meta-data The Instance Metadata Query tool allows you to query the instance metadata without having to type out the full URI or category names The EC2 config service or batch command are not suitable for accessing this information References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

- ✅ Download and run the Instance Metadata Query Tool

Explanation:-This information is stored in the instance metadata on the instance. You can access the instance metadata through a URI or by using the Instance Metadata Query tool The instance metadata is available at http://169.254.169.254/latest/meta-data The Instance Metadata Query tool allows you to query the instance metadata without having to type out the full URI or category names The EC2 config service or batch command are not suitable for accessing this information References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

- Use the Batch command

Q21) A solutions architect is building a scalable and fault tolerant web architecture and is evaluating the benefits of the Elastic Load Balancing (ELB) service. Which statements are true regarding ELBs? (select 2)

- Both types of ELB route traffic to the public IP addresses of EC2 instances
- ✅ Internet facing ELB nodes have public IPs

Explanation:-Internet facing ELB nodes have public IPs Both types of ELB route traffic to the private IP addresses of EC2 instances For public facing ELBs you must have one public subnet in each AZ where the ELB is defined Internal-only load balancers do not require an Internet gateway Only 1 subnet per AZ can be enabled for each ELB References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- Multiple subnets per AZ can be enabled for each ELB
- ✅ For public facing ELBs you must have one public subnet in each AZ where the ELB is defined

Explanation:-Internet facing ELB nodes have public IPs Both types of ELB route traffic to the private IP addresses of EC2 instances For public facing ELBs you must have one public subnet in each AZ where the ELB is defined Internal-only load balancers do not require an Internet gateway Only 1 subnet per AZ can be enabled for each ELB References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q22)

A Solutions Architect is designing the messaging and streaming layers of a serverless application. The messaging layer will manage communications between components and the streaming layer will manage real-time analysis and processing of streaming data.The Architect needs to select the most appropriate AWS services for these functions.

Which services should be used for the messaging and streaming layers? (choose 2)

- ✅ Use Amazon Kinesis for collecting, processing and analyzing real-time streaming data

Explanation:-Amazon Kinesis makes it easy to collect, process, and analyze real-time streaming data. With Amazon Kinesis Analytics, you can run standard SQL or build entire streaming applications using SQL Amazon Simple Notification Service (Amazon SNS) provides a fully managed messaging service for pub/sub patterns using asynchronous event notifications and mobile push notifications for microservices, distributed systems, and serverless applications Amazon Elastic Map Reduce runs on EC2 instances so is not serverless Amazon Simple Workflow Service is used for executing tasks not sending messages Amazon CloudTrail is used for recording API activity on your account References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/

- Use Amazon CloudTrail for collecting, processing and analyzing real-time streaming data
- Use Amazon EMR for collecting, processing and analyzing real-time streaming data
- ✅ Use Amazon SNS for providing a fully managed messaging service

Explanation:-Amazon Kinesis makes it easy to collect, process, and analyze real-time streaming data. With Amazon Kinesis Analytics, you can run standard SQL or build entire streaming applications using SQL Amazon Simple Notification Service (Amazon SNS) provides a fully managed messaging service for pub/sub patterns using asynchronous event notifications and mobile push notifications for microservices, distributed systems, and serverless applications Amazon Elastic Map Reduce runs on EC2 instances so is not serverless Amazon Simple Workflow Service is used for executing tasks not sending messages Amazon CloudTrail is used for recording API activity on your account References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/

Q23)

Using the VPC wizard, you have selected the option “VPC with Public and Private Subnets and Hardware VPN access??.

Which of the statements below correctly describe the configuration that will be created? (choose 2)

- ✅ A virtual private gateway will be created

Explanation:-The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet, and a virtual private gateway to enable communication with your own network over an IPsec VPN tunnel Review the scenario described in the AWS article below for more information References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/ https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html

- A NAT gateway will be created for the private subnet
- A peering connection will be made between the public and private subnets
- ✅ One subnet will be connected to your corporate data center using an IPSec VPN tunnel

Explanation:-The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet, and a virtual private gateway to enable communication with your own network over an IPsec VPN tunnel Review the scenario described in the AWS article below for more information References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/ https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html

---

Q24) You are building a small web application running on EC2 that will be serving static content. The user base is spread out globally and speed is important. Which AWS service can deliver the best user experience cost-effectively and reduce the load on the web server?

- Amazon S3
- ✅ Amazon CloudFront

Explanation:-This is a good use case for CloudFront as the user base is spread out globally and CloudFront can cache the content closer to users and also reduce the load on the web server running on EC2 Amazon S3 is very cost-effective however a bucket is located in a single region and therefore performance is EBS is not the most cost-effective storage solution and the data would be located in a single region to latency could be an issue Amazon RedShift is a data warehouse and is not suitable in this solution References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Amazon RedShift
- Amazon EBS volume

Q25) You are using CloudWatch to monitor the performance of AWS Lambda. Which metrics does Lambda track? (choose 2)

✅ Total number of requests

Explanation:-Lambda automatically monitors Lambda functions and reports metrics through CloudWatch. Lambda tracks the number of requests, the latency per request, and the number of requests resulting in an error You can view the request rates and error rates using the AWS Lambda Console, the CloudWatch console, and other AWS resources References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/

⚪ Total number of connections

⚪ Total number of transactions

✅ Latency per request

Explanation:-Lambda automatically monitors Lambda functions and reports metrics through CloudWatch. Lambda tracks the number of requests, the latency per request, and the number of requests resulting in an error You can view the request rates and error rates using the AWS Lambda Console, the CloudWatch console, and other AWS resources References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/

Q26) Which AWS service does API Gateway integrate with to enable users from around the world to achieve the lowest possible latency for API requests and responses?

⚪ Lambda

✅ CloudFront

Explanation:-CloudFront is used as the public endpoint for API Gateway and provides reduced latency and distributed denial of service protection through the use of CloudFront Direct Connect provides a private network into AWS from your data center S3 Transfer Acceleration is not used with API Gateway, it is used to accelerate uploads of S3 objects Lambda is not used to reduce latency for API requests References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

⚪ S3 Transfer Acceleration

⚪ Direct Connect

Q27)

A Solutions Architect is creating a design for a multi-tiered web application. The application will use multiple AWS services and must be designed with elasticity and high-availability in mind.

Which architectural best practices should be followed to reduce interdependencies between systems? (choose 2)

⚪ Implement service discovery using static IP addresses

✅ Enable graceful failure through AWS Auto Scaling

Explanation:-ul> Asynchronous integration - this is another form of loose coupling where an interaction does not need an immediate response (think SQS queue or Kinesis) Graceful failure - build applications such that they handle failure in a graceful manner (reduce the impact of failure and implement retries). Auto Scaling helps to reduce the impact of failure by launching replacement instances Well-defined interfaces - reduce interdependencies in a system by enabling interaction only through specific, technology-agnostic interfaces (e.g. RESTful APIs). A relational database is not an example of a well-defined interface Service discovery - disparate resources must have a way of discovering each other without prior knowledge of the network topology. Usually DNS names and a method of resolution are preferred over static IP addresses which need to be hardcoded somewhere Though automatic scaling for storage and database provides scalability (not necessarily elasticity), it does not reduce interdependencies between systems References: https://aws.amazon.com/architecture/well-architected/

⚪ Enable automatic scaling for storage and databases

✅ Implement asynchronous integration using Amazon SQS queues

Explanation:-ul> Asynchronous integration - this is another form of loose coupling where an interaction does not need an immediate response (think SQS queue or Kinesis) Graceful failure - build applications such that they handle failure in a graceful manner (reduce the impact of failure and implement retries). Auto Scaling helps to reduce the impact of failure by launching replacement instances Well-defined interfaces - reduce interdependencies in a system by enabling interaction only through specific, technology-agnostic interfaces (e.g. RESTful APIs). A relational database is not an example of a well-defined interface Service discovery - disparate resources must have a way of discovering each other without prior knowledge of the network topology. Usually DNS names and a method of resolution are preferred over static IP addresses which need to be hardcoded somewhere Though automatic scaling for storage and database provides scalability (not necessarily elasticity), it does not reduce interdependencies between systems References: https://aws.amazon.com/architecture/well-architected/

Q28) You are using encrypted Amazon Elastic Block Store (EBS) volumes with your instances in EC2. A security administrator has asked how encryption works with EBS. Which statements are correct? (choose 2)

✅ Data in transit between an instance and an encrypted volume is also encrypted

Explanation:-All EBS types support encryption and all instance families now support encryption Not all instance types support encryption Data in transit between an instance and an encrypted volume is also encrypted (data is encrypted in trans You can have encrypted an unencrypted EBS volumes attached to an instance at the same time Snapshots of encrypted volumes are encrypted automatically EBS volumes restored from encrypted snapshots are encrypted automatically EBS volumes created from encrypted snapshots are also encrypted References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

✅ Encryption is supported on all Amazon EBS volume types

Explanation:-All EBS types support encryption and all instance families now support encryption Not all instance types support encryption Data in transit between an instance and an encrypted volume is also encrypted (data is encrypted in trans You can have encrypted an unencrypted EBS volumes attached to an instance at the same time Snapshots of encrypted volumes are encrypted automatically EBS volumes restored from encrypted snapshots are encrypted automatically EBS volumes created from encrypted snapshots are also encrypted References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

⚪ Volumes created from encrypted snapshots are unencrypted

⚪ Data is only encrypted at rest

Q29)

A systems integration consultancy regularly deploys and manages multi-tiered web services for customers on AWS. The SysOps team are facing challenges in tracking changes that are made to the web services and rolling back when problems occur.

Which of the approaches below would BEST assist the SysOps team?

✅ Use CloudFormation templates to deploy and manage the web services

Explanation:-When you provision your infrastructure with AWS CloudFormation, the AWS CloudFormation template describes exactly what resources are provisioned and their settings. Because these templates are text files, you simply track differences in your templates to track changes to your infrastructure, similar to the way developers control revisions to source code. For example, you can use a version control system with your templates so that you know exactly what changes were made, who made them, and when. If at any point you need to reverse changes to your infrastructure, you can use a previous version of your template AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. However, CloudFormation would be the preferred method of maintaining the state of the overall architecture AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda function AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices References: https://aws.amazon.com/cloudformation/resources/

- Use AWS Systems Manager to manage all updates to the web services
- Use Trusted Advisor to record updates made to the web services
- Use CodeDeploy to manage version control for the web services

---

Q30)

You are developing some code that uses a Lambda function and you would like to enable the function to connect to an ElastiCache cluster within a VPC that you own.

What VPC-specific information must you include in your function to enable this configuration? (choose 2)

- VPC Peering IDs
- ✅ VPC Subnet IDs

Explanation:-To enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs. AWS Lambda uses this information to set up elastic network interfaces (ENIs) that enable your function Please see the AWS article linked below for more details on the requirements References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/ https://docs.aws.amazon.com/lambda/latest/dg/vpc.html

- VPC Route Table IDs
- ✅ VPC Security Group IDs

Explanation:-To enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs. AWS Lambda uses this information to set up elastic network interfaces (ENIs) that enable your function Please see the AWS article linked below for more details on the requirements References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/ https://docs.aws.amazon.com/lambda/latest/dg/vpc.html

---

Q31)

There is a temporary need to share some video files that are stored in a private S3 bucket. The consumers do not have AWS accounts and you need to ensure that only authorized consumers can access the files.

What is the best way to enable this access?

- ✅ Generate a pre-signed URL and distribute it to the consumers

Explanation:-S3 pre-signed URLs can be used to provide temporary access to a specific object to those who do not have AWS credentials. This is the best option Enabling public read access does not restrict the content to authorized consumers You cannot use CloudFront as hash tags are not a CloudFront authentication mechanism Security Groups do not apply to S3 buckets References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Use CloudFront to distribute the files using authorization hash tags
- Enable public read access for the S3 bucket
- Configure an allow rule in the Security Group for the IP addresses of the consumers

---

Q32)

A Solutions Architect is deploying an Auto Scaling Group (ASG) and needs to determine what CloudWatch monitoring option to use.

Which of the statements below would assist the Architect in making his decision? (choose 2)

- Basic monitoring is enabled by default if the ASG is created from the CLI
- ✅ Detailed monitoring is enabled by default if the ASG is created from the CLI

Explanation:-Basic monitoring sends EC2 metrics to CloudWatch about ASG instances every 5 minutes Detailed can be enabled and sends metrics every 1 minute (it is always chargeable) When the launch configuration is created from the CLI detailed monitoring of EC2 instances is enabled by default When you enable Auto Scaling group metrics, Auto Scaling sends sampled data to CloudWatch every minute. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- ✅ Basic monitoring is enabled by default if the ASG is created from the console

Explanation:-Basic monitoring sends EC2 metrics to CloudWatch about ASG instances every 5 minutes Detailed can be enabled and sends metrics every 1 minute (it is always chargeable) When the launch configuration is created from the CLI detailed monitoring of EC2 instances is enabled by default When you enable Auto Scaling group metrics, Auto Scaling sends sampled data to CloudWatch every minute. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- Detailed monitoring is chargeable and must always be manually enabled

---

Q33)

An application you are designing receives and processes files. The files are typically around 4GB in size and the application extracts metadata from the files which typically takes a few seconds for each file. The pattern of updates is highly dynamic with times of little activity and then multiple uploads within a short period of time.

What architecture will address this workload the most cost efficiently?

- Store the file in an EBS volume which can then be accessed by another EC2 instance for processing
- Place the files in an SQS queue, and use a fleet of EC2 instances to extract the metadata
- ✅ Upload files into an S3 bucket, and use the Amazon S3 event notification to invoke a Lambda function to extract the metadata

Explanation:-Storing the file in an S3 bucket is cost-efficient, and using S3 event notifications to invoke a Lambda function works well for this unpredictable workload and is cost-efficient Kinesis data streams consumers run on EC2 instances (not Lambda) SQS queues have a maximum message size of 256KB. You can use the extended client library for Java to use pointers to a payload on S3 but the maximum payload size is 2GB Storing the file in an EBS volume and using EC2 instances for processing is not cost efficient. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/ https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html

- Use a Kinesis data stream to store the file, and use Lambda for processing

---

Q34)

A Solutions Architect is developing a mobile web app that will provide access to health related data. The web apps will be tested on Android and iOS devices. The Architect needs to run tests on multiple devices simultaneously and to be able to reproduce issues, and record logs and performance data to ensure quality before release.

What AWS service can be used for these requirements?

- AWS Workspaces
- ✅ AWS Device Farm

Explanation:-AWS Device Farm is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. It is not used for testing Amazon WorkSpaces is a managed, secure cloud desktop service Amazon AppStream 2.0 is a fully managed application streaming service References: https://aws.amazon.com/device-farm/

- AWS Cognito
- Amazon Appstream 2.0

Q35)

A Solutions Architect is designing a highly-scalable system to track records. Records must remain available for immediate download for three months, and then the records must be deleted.

What's the most appropriate decision for this use case?

- Store the files on Amazon EFS, and create a lifecycle policy to remove the files after three months
- Store the files on Amazon Glacier, and create a lifecycle policy to remove the files after three months
- ✅ Store the files on Amazon S3, and create a lifecycle policy to remove the files after three months

Explanation:-With S3 you can create a lifecycle action using the "expiration action element" which expires objects (deletes them) at the specified time S3 lifecycle actions apply to any storage class, including Glacier, however Glacier would not allow immediate download There is no lifecycle policy available for deleting files on EBS and EFS NOTE: The new Amazon Data Lifecycle Manager (DLM) feature automates the creation, retention, and deletion of EBS snapshots but not the individual files within an EBS volume. This is a new feature that may not yet feature on the exam References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Store the files on Amazon EBS, and create a lifecycle policy to remove the files after three months

---

Q36)

You just created a new subnet in your VPC and have launched an EC2 instance into it. You are trying to directly access the EC2 instance from the Internet and cannot connect.

Which steps should you take to troubleshoot the issue? (choose 2)

- Check that there is a NAT Gateway configured for the subnet
- ✅ Check that the route table associated with the subnet has an entry for an Internet Gateway

Explanation:-Public subnets are subnets that have: - “Auto-assign public IPv4 address?? set to “Yes?? - The subnet route table has an attached Internet Gateway A NAT Gateway is used for providing outbound Internet access for EC2 instances in private subnets Checking you can ping from another subnet does not relate to being able to access the instance remotely as it uses different protocols and a different network path Security groups are stateful and do not need a rule for outbound traffic. For this solution you would only need to create an inbound rule that allows the relevant protocol References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Check that you can ping the instance from another subnet
- ✅ Check that the instance has a public IP address

Explanation:-Public subnets are subnets that have: - “Auto-assign public IPv4 address?? set to “Yes?? - The subnet route table has an attached Internet Gateway A NAT Gateway is used for providing outbound Internet access for EC2 instances in private subnets Checking you can ping from another subnet does not relate to being able to access the instance remotely as it uses different protocols and a different network path Security groups are stateful and do not need a rule for outbound traffic. For this solution you would only need to create an inbound rule that allows the relevant protocol References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q37) The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. According to the policy, what is AWS's position on penetration testing?

- AWS allow penetration testing for all resources
- AWS allow penetration testing by customers on their own VPC resources
- ✅ AWS allow penetration for some resources with prior authorization

Explanation:-Permission is required for all penetration tests You must complete and submit the AWS Vulnerability / Penetration Testing Request Form to request authorization for penetration testing to or originating from any AWS resources There is a limited set of resources on which penetration testing can be performed References: https://aws.amazon.com/security/penetration-testing/

- AWS do not allow any form of penetration testing

Q38)

A company is moving some unstructured data into AWS and a Solutions Architect has created a bucket named "contosocustomerdata" in the ap-southeast-2 region.

Which of the following bucket URLs would be valid for accessing the bucket? (choose 2)

- https://s3-ap-southeast-2.amazonaws.com.contosocustomerdata
- ✅ https://s3-ap-southeast-2.amazonaws.com/contosocustomerdata

Explanation:-AWS supports S3 URLs in the format of https://.s3.amazonaws.com

- ✅ https://contosocustomerdata.s3.amazonaws.com

Explanation:-AWS supports S3 URLs in the format of https://.s3.amazonaws.com

- https://amazonaws.s3-ap-southeast-2.com/contosocustomerdata

---

Q39)

An Amazon CloudWatch alarm recently notified you that the load on a DynamoDB table you are running is getting close to the provisioned capacity for writes. The DynamoDB table is part of a two-tier customer-facing application. You are concerned about what will happen if the limit is reached but need to wait for approval to increase the WriteCapacityUnits value assigned to the table.

What will happen if the limit for the provisioned capacity for writes is reached?

- The requests will succeed, and an HTTP 200 status code will be returned
- The requests will be throttled, and fail with an HTTP 503 code (Service Unavailable)
- DynamoDB scales automatically so there's no need to worry
- ✅ The requests will be throttled, and fail with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceededException

Explanation:-DynamoDB can throttle requests that exceed the provisioned throughput for a table. When a request is throttled it fails with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceeded exception (not a 503 or 200 status code) When using the provisioned capacity pricing model DynamoDB does not automatically scale. DynamoDB can automatically scale when using the new on-demand capacity mode (DynamoDB Auto Scaling) however this is not configured for this database References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

Q40) To increase the resiliency of your RDS DB instance, you decided to enable Multi-AZ. Where will the new standby RDS instance be created?

- In a different AWS Region to protect against Region failures
- In another subnet within the same AZ
- ✅ In the same AWS Region but in a different AZ for high availability

Explanation:-Multi-AZ RDS creates a replica in another AZ within the same region and synchronously replicates to it (DR only). You cannot choose which AZ in the region will be chosen to create the standby DB instance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- You must specify the location when configuring Multi-AZ

Q41)

A Solutions Architect is considering the best approach to enabling Internet access for EC2 instances in a private subnet.

What advantages do NAT Gateways have over NAT Instances? (choose 2)

- Can be assigned to security groups
- ✅ Managed for you by AWS

Explanation:-NAT gateways are managed for you by AWS. NAT gateways are highly available in each AZ into which they are deployed. They are not associated with any security groups and can scale automatically up to 45Gbps NAT instances are managed by you. They must be scaled manually and do not provide HA. NAT Instances can be used as bastion hosts and can be assigned to security groups References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Can be used as a bastion host
- ✅ Highly available within each AZ

Explanation:-NAT gateways are managed for you by AWS. NAT gateways are highly available in each AZ into which they are deployed. They are not associated with any security groups and can scale automatically up to 45Gbps NAT instances are managed by you. They must be scaled manually and do not provide HA. NAT Instances can be used as bastion hosts and can be assigned to security groups References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q42) Your manager has asked you to explain the benefits of using IAM groups. Which of the below statements are valid benefits? (choose 2)

- Provide the ability to nest groups to create an organizational hierarchy
- ✅ Enables you to attach IAM permission policies to more than one user at a time

Explanation:-Groups are collections of users and have policies attached to them. A group is not an identity and cannot be identified as a principal in an IAM policy. Use groups to assign permissions to users. Use the principal of least privilege when assigning permissions. You cannot nest groups (groups within groups) You cannot use groups to restrict access to subnet in your VPC Custom permission policies are created using IAM policies. These are then attached to users, groups or roles References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

- Provide the ability to create custom permission policies
- ✅ Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users

Explanation:-Groups are collections of users and have policies attached to them. A group is not an identity and cannot be identified as a principal in an IAM policy. Use groups to assign permissions to users. Use the principal of least privilege when assigning permissions. You cannot nest groups (groups within groups) You cannot use groups to restrict access to subnet in your VPC Custom permission policies are created using IAM policies.

These are then attached to users, groups or roles References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

Q43) You would like to implement a method of automating the the creation, retention, and deletion of backups for the EBS volumes in your VPC. What is the easiest way to automate these tasks using AWS tools?

- Create a scheduled job and run the AWS CLI command “create-snapshot"
- Create a scheduled job and run the AWS CLI command “create-backup"
- ✅ Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes

Explanation:-You backup EBS volumes by taking snapshots. This can be automated via the AWS CLI command "create-snapshot". However the question is asking for a way to automate not just the creation of the snapshot but the retention and deletion too. The EBS Data Lifecycle Manager (DLM) is a new feature that can automate all of these actions for you and this can be performed centrally from within the management console Snapshots capture a point-in-time state of an instance and are stored on Amazon S3. They do not provide granular backup (not a replacement for backup software) You cannot configure volume replication for EBS volumes using AWS tools References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html https://docs.aws.amazon.com/cli/latest/reference/ec2/create-snapshot.html

- Configure EBS volume replication to create a backup on S3

Q44) An application has been deployed in a private subnet within your VPC and an ELB will be used to accept incoming connections. You need to setup the configuration for the listeners on the ELB.When using a Classic Load Balancer, which of the following combinations of listeners support the proxy protocol? (choose 2)

- ✅ Front-End – TCP & Back-End – TCP

Explanation:-The proxy protocol only applies to L4 and the back-end listener must be TCP for proxy protocol When using the proxy protocol the front-end listener can be either TCP or SSL The X-forwarded-for header only applies to L7 Proxy protocol for TCP/SSL carries the source (client) IP/port information. 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 connection References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/using-elb-listenerconfig-quickref.html

- Front-End – SSL & Back-End – SSL
- Front-End – HTTP & Back-End SSL
- ✅ Front-End – SSL & Back-End - TCP

Explanation:-The proxy protocol only applies to L4 and the back-end listener must be TCP for proxy protocol When using the proxy protocol the front-end listener can be either TCP or SSL The X-forwarded-for header only applies to L7 Proxy protocol for TCP/SSL carries the source (client) IP/port information. 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 connection References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/ https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/using-elb-listenerconfig-quickref.html

---

Q45)

You have created a VPC with private and public subnets and will be deploying a new mySQL database server running on an EC2 instance.

Which subnet should you deploy the database server into?

- The subnet that is mapped to the primary AZ in the region
- The public subnet
- It doesn’t matter
- ✅ The private subnet

Explanation:-AWS best practice is to deploy databases into private subnets wherever possible. You can then deploy your web front-ends into public subnets and configure these, or an additional application tier to write data to the database Public subnets are typically used for web front-ends as they are directly accessible from the Internet. It is preferable to launch your database in a private subnet There is no such thing as a "primary" Availability Zone (AZ). All AZs are essentially created equal and your subnets map 1:1 to a single AZ References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q46) You just attempted to restart a stopped EC2 instance and it immediately changed from a pending state to a terminated state. What are the most likely explanations? (choose 2)

- ✅ An EBS snapshot is corrupt

Explanation:-The following are a few reasons why an instance might immediately terminate: - You've reached your EBS volume limit - An EBS snapshot is corrupt - The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption - The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file) It is possible that an instance type is not supported by an AMI and this can cause an "UnsupportedOperation" client error. However, in this case the instance was previously running (it is in a stopped state) so it is unlikely that this is the issue If AWS does not have capacity available a InsufficientInstanceCapacity error will be generated when you try to launch a new instance or restart a stopped instance If you've reached the limit on the number of instances you can launch in a region you get an InstanceLimitExceeded error when you try to launch a new instance or restart a stopped instance References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html

- You have reached the limit on the number of instances that you can launch in a region
- AWS does not currently have enough available On-Demand capacity to service your request
- ✅ You've reached your EBS volume limit

Explanation:-The following are a few reasons why an instance might immediately terminate: - You've reached your EBS volume limit - An EBS snapshot is corrupt - The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption - The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file) It is possible that an instance type is not supported by an AMI and this can cause an "UnsupportedOperation" client error. However, in this case the instance was previously running (it is in a stopped state) so it is unlikely that this is the issue If AWS does not have capacity available a InsufficientInstanceCapacity error will be generated when you try to launch a new instance or restart a stopped instance If you've reached the limit on the number of instances you can launch in a region you get an InstanceLimitExceeded error when you try to launch a new instance or restart a stopped instance References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html

---

Q47)

You have a requirement to perform a large-scale testing operation that will assess the ability of your application to scale. You are planning on deploying a large number of c3.2xlarge instances with several PIOPS EBS volumes attached to each. You need to ensure you don't run into any problems with service limits.

What are the service limits you need to be aware of in this situation?

- 20 On-Demand EC2 instances and 100,000 aggregate PIOPS per region
- 20 On-Demand EC2 instances and 300 TiB of aggregate PIOPS volume storage per account
- ✅ 20 On-Demand EC2 instances and 300 TiB of aggregate PIOPS volume storage per region

Explanation:-You are limited to running up to a total of 20 On-Demand instances across the instance family, purchasing 20 Reserved Instances, and requesting Spot Instances per your dynamic spot limit per region (by default) You are limited to an aggregate of 300 TiB of aggregate PIOPS volumes per region and 300,000 aggregate PIOPS References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

- 20 On-Demand EC2 instances and 100,000 aggregate PIOPS per account

---

Q48)

A Solutions Architect needs to attach an Elastic Network Interface (ENI) to an EC2 instance. This can be performed when the instance is in different states.

What state does "warm attach?? refer to?

- Attaching an ENI to an instance when it is running
- Attaching an ENI to an instance during the launch process
- ✅ Attaching an ENI to an instance when it is stopped

Explanation:-ENIs can be "hot attached?? to running instances ENIs can be "warm-attached?? when the instance is stopped ENIs can be "cold-attached?? when the instance is launched References: https://digitalcloud.guru/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

- Attaching an ENI to an instance when it is idle

Q49)

A client has requested a recommendation for a high-level hosting architecture for a distributed application that will utilize decoupled components.The application will make use of servers running on EC2 instances and in the client's own data centers. Which AWS application integration services could you use to support interaction between the servers?

Which of the following options are valid? (choose 2)

- ✅ Amazon SWF

Explanation:-Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks Amazon 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 A VPC is a logical network construct Amazon S3 is an object store and is not designed for application integration between servers Amazon DynamoDB is a non-relational database References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-swf/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/

- Amazon S3
- ✅ Amazon SQS

Explanation:-Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks Amazon 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 A VPC is a logical network construct Amazon S3 is an object store and is not designed for application integration between servers Amazon DynamoDB is a non-relational database References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-swf/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/

- Amazon VPC

Q50)

A Solutions Architect has setup a VPC with a public subnet and a VPN-only subnet. The public subnet is associated with a custom route table that has a route to an Internet Gateway. The VPN-only subnet is associated with the main route table and has a route to a virtual private gateway. The Architect has created a new subnet in the VPC and launched an EC2 instance in it. However, the instance cannot connect to the Internet.

What is the MOST likely reason?

- The new subnet has not been associated with a route table
- The Internet Gateway is experiencing connectivity problems
- There is no NAT Gateway available in the new subnet so Internet connectivity is not possible
- ✅ The subnet has been automatically associated with the main route table which does not have a route to the Internet

Explanation:-When you create a new subnet, it is automatically associated with the main route table. Therefore, the EC2 instance will not have a route to the Internet. The Architect should associate the new subnet with the custom route table NAT Gateways are used for connecting EC2 instances in private subnets to the Internet. This is a valid reason for a private subnet to not have connectivity, however in this case the Architect is attempting to use an Internet Gateway Subnets are always associated to a route table when created Internet Gateways are highly-available so it's unlikely that IGW connectivity is the issue References: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

---