Answer Sheet

Q1)

An issue has been raised to you whereby a client is concerned about the permissions assigned to his containerized applications. The containers are using the EC2 launch type. The current configuration uses the container instance's IAM roles for assigning permissions to the containerized applications.

The client has asked if it's possible to implement more granular permissions so that some applications can be assigned more restrictive permissions?

- This can be achieved by configuring a resource-based policy for each application
- This cannot be changed as IAM roles can only be linked to container instances
- ✅ This can be achieved using IAM roles for tasks, and splitting the containers according to the permissions required to different task definition profiles

Explanation:-With IAM roles for Amazon ECS tasks, you can specify an IAM role that can be used by the containers in a task. Using this feature you can achieve the required outcome by using IAM roles for tasks and splitting the containers according to the permissions required to different task profiles. The solution can be achieved whether using the EC2 or Fargate launch types Amazon ECS does not support IAM resource-based policies References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/ https://docs.aws.amazon.com/AmazonECS/latest/userguide/task-iam-roles.html https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

- This can only be achieved using the Fargate launch type

Q2)

An application you are designing will gather data from a website hosted on an EC2 instance and write the data to an S3 bucket. The application will use API calls to interact with the EC2 instance and S3 bucket.

Which access control strategy will be the the MOST operationally efficient? (choose 2)

- ✅ Create an IAM policy

Explanation:-Policies are documents that define permissions and can be applied to users, groups and roles. Policy documents are written in JSON (key value pair that consists of an attribute and a value) Within an IAM policy you can grant either programmatic access or AWS Management Console access to Amazon S3 resources Key pairs are used for access to EC2 instances; a bucket policy would not assist with access control with EC2 and granting management console access will not assist the application which is making API calls to the services AWS recommend using IAM policies instead of S3 bucket policies in the following circumstances: You need to control access to AWS services other than S3. IAM policies will be easier to manage since you can centrally manage all of your permissions in IAM, instead of spreading them between IAM and S3 You have numerous S3 buckets each with different permissions requirements. IAM policies will be easier to manage since you don't have to define a large number of S3 bucket policies and can instead rely on fewer, more detailed IAM policies You prefer to keep access control policies in the IAM environment References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/ https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s3-resources/

- Grant AWS Management Console access
- ✅ Grant programmatic access

Explanation:-Policies are documents that define permissions and can be applied to users, groups and roles. Policy documents are written in JSON (key value pair that consists of an attribute and a value) Within an IAM policy you can grant either programmatic access or AWS Management Console access to Amazon S3 resources Key pairs are used for access to EC2 instances; a bucket policy would not assist with access control with EC2 and granting management console access will not assist the application which is making API calls to the services AWS recommend using IAM policies instead of S3 bucket policies in the following circumstances: You need to control access to AWS services other than S3. IAM policies will be easier to manage since you can centrally manage all of your permissions in IAM, instead of spreading them between IAM and S3 You have numerous S3 buckets each with different permissions requirements. IAM policies will be easier to manage since you don't have to define a large number of S3 bucket policies and can instead rely on fewer, more detailed IAM policies You prefer to keep access control policies in the IAM environment References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/ https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s3-resources/

- Ue key pairs

Q3)

A three-tier application running in your VPC uses Auto Scaling for maintaining a desired count of EC2 instances. One of the EC2 instances just reported an EC2 Status Check status of Impaired.

Once this information is reported to Auto Scaling, what action will be taken?

- ✅ The impaired instance will be terminated, then a replacement will be launched

Explanation:-By default Auto Scaling uses EC2 status checks Unlike AZ rebalancing, termination of unhealthy instances happens first, then Auto Scaling attempts to launch new instances to replace terminated instances Auto Scaling does not wait for the health check grace period or verify with ELB before taking any action References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

- A new instance will immediately be launched, then the impaired instance will be terminated
- Auto Scaling waits for the health check grace period and then terminates the instance
- Auto Scaling must verify with the ELB status checks before taking any action

---

Q4)

You work for a large multinational retail company. The company has a large presence in AWS in multiple regions. You have established a new office and need to implement a high-bandwidth, low-latency connection to multiple VPCs in multiple regions within the same account. The VPCs each have unique CIDR ranges.

What would be the optimum solution design using AWS technology? (choose 2)

✅ Create a Direct Connect gateway, and create private VIFs to each region

Explanation:-You should implement an AWS Direct Connect connection to the closest region. You can then use Direct Connect gateway to create private virtual interfaces (VIFs) to each AWS region. Direct Connect gateway provides a grouping of Virtual Private Gateways (VGWs) and Private Virtual Interfaces (VIFs) that belong to the same AWS account and enables you to interface with VPCs in any AWS Region (except AWS China Region). You can share a private virtual interface to interface with more than one Virtual Private Cloud (VPC) reducing the number of BGP sessions required You do not need to implement multiple Direct Connect connections to each region. This would be a more expensive option as you would need to pay for an international private connection AWS VPN CloudHub is not the best solution as you have been asked to implement high-bandwidth, low-latency connections and VPN uses the Internet so is not reliable An MPLS network could be used to create a network topology that gets you closer to AWS in each region but you would still need use Direct Connect or VPN for the connectivity into AWS. Also, the question states that you should use AWS technology and MPLS is not offered as a service by AWS References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/

⚪ Implement Direct Connect connections to each AWS region

⚪ Configure AWS VPN CloudHub

✅ Implement a Direct Connect connection to the closest AWS region

Explanation:-You should implement an AWS Direct Connect connection to the closest region. You can then use Direct Connect gateway to create private virtual interfaces (VIFs) to each AWS region. Direct Connect gateway provides a grouping of Virtual Private Gateways (VGWs) and Private Virtual Interfaces (VIFs) that belong to the same AWS account and enables you to interface with VPCs in any AWS Region (except AWS China Region). You can share a private virtual interface to interface with more than one Virtual Private Cloud (VPC) reducing the number of BGP sessions required You do not need to implement multiple Direct Connect connections to each region. This would be a more expensive option as you would need to pay for an international private connection AWS VPN CloudHub is not the best solution as you have been asked to implement high-bandwidth, low-latency connections and VPN uses the Internet so is not reliable An MPLS network could be used to create a network topology that gets you closer to AWS in each region but you would still need use Direct Connect or VPN for the connectivity into AWS. Also, the question states that you should use AWS technology and MPLS is not offered as a service by AWS References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/

Q5) A Solutions Architect is designing a front-end that accepts incoming requests for back-end business logic applications. The Architect is planning to use Amazon API Gateway, which statements are correct in relation to the service? (choose 2)

✅ API Gateway is a collection of resources and methods that are integrated with back-end HTTP endpoints, Lambda functions or other AWS services

Explanation:-An Amazon API Gateway is a collection of resources and methods that are integrated with back-end HTTP endpoints, Lambda function or other AWS services. API Gateway handles all of the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls. Throttling can be configured at multiple levels including Global and Service Call CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds Direct Connect is a network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS DynamoDB uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

⚪ API Gateway uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns

⚪ API Gateway is a network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS

✅ Throttling can be configured at multiple levels including Global and Service Call

Explanation:-An Amazon API Gateway is a collection of resources and methods that are integrated with back-end HTTP endpoints, Lambda function or other AWS services. API Gateway handles all of the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls. Throttling can be configured at multiple levels including Global and Service Call CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds Direct Connect is a network service that provides an alternative to using the Internet to connect customers' on-premise sites to AWS DynamoDB uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

Q6)

The Perfect Forward Secrecy (PFS) security feature uses a derived session key to provide additional safeguards against the eavesdropping of encrypted data.

Which two AWS services support PFS? (choose 2)

⚪ Auto Scaling

⚪ EC2

✅ CloudFront

Explanation:-CloudFront and ELB support Perfect Forward Secrecy which creates a new private key for each SSL session Perfect Forward Secrecy (PFS) provides additional safeguards against the eavesdropping of encrypted data, through the use of a unique random session key The other services listed do not support PFS 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/

✅ Elastic Load Balancing

Explanation:-CloudFront and ELB support Perfect Forward Secrecy which creates a new private key for each SSL session Perfect Forward Secrecy (PFS) provides additional safeguards against the eavesdropping of encrypted data, through the use of a unique random session key The other services listed do not support PFS 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/

Q7) You have been asked to review the security posture of your EC2 instances in AWS. When reviewing security groups, which rule types do you need to inspect? (choose 2)

⚪ Stateless

✅ Outbound

Explanation:-Security Groups can be configured with Inbound (ingress) and Outbound (egress) rules. You can only assign permit rules in a security group, You cannot assign deny rules and all rules are evaluated until a permit is encountered or continues until the implicit deny Security groups are stateful (whereas Network ACLs are stateless) and this is not something that is configured in a rule References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Stateful
- ✅ Inbound

Explanation:-Security Groups can be configured with Inbound (ingress) and Outbound (egress) rules. You can only assign permit rules in a security group, You cannot assign deny rules and all rules are evaluated until a permit is encountered or continues until the implicit deny Security groups are stateful (whereas Network ACLs are stateless) and this is not something that is configured in a rule References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q8)

An application you manage exports data from a relational database into an S3 bucket. The data analytics team wants to import this data into a RedShift cluster in a VPC in the same account. Due to the data being sensitive the security team has instructed you to ensure that the data traverses the VPC without being routed via the public Internet.

Which combination of actions would meet this requirement? (choose 2)

- Create a NAT gateway in a public subnet to allows the Amazon RedShift cluster to access Amazon S3
- ✅ Enable Amazon RedShift Enhanced VPC routing

Explanation:-Amazon RedShift Enhanced VPC routing forces all COPY and UNLOAD traffic between clusters and data repositories through a VPC Implementing an S3 VPC endpoint will allow S3 to be accessed from other AWS services without traversing the public network. Amazon S3 uses the Gateway Endpoint type of VPC endpoint with which a target for a specified route is entered into the VPC route table and used for traffic destined to a supported AWS service Cluster Security Groups are used with RedShift on EC2-Classic VPCs, regular security groups are used in EC2-VPC A NAT Gateway is used to allow instances in a private subnet to access the Internet and is of no use in this situation References: https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Set up a NAT gateway in a private subnet to allow the Amazon RedShift cluster to access Amazon S3
- ✅ Create and configure an Amazon S3 VPC endpoint

Explanation:-Amazon RedShift Enhanced VPC routing forces all COPY and UNLOAD traffic between clusters and data repositories through a VPC Implementing an S3 VPC endpoint will allow S3 to be accessed from other AWS services without traversing the public network. Amazon S3 uses the Gateway Endpoint type of VPC endpoint with which a target for a specified route is entered into the VPC route table and used for traffic destined to a supported AWS service Cluster Security Groups are used with RedShift on EC2-Classic VPCs, regular security groups are used in EC2-VPC A NAT Gateway is used to allow instances in a private subnet to access the Internet and is of no use in this situation References: https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q9) A Solutions Architect is creating a new VPC and is creating a security group and network ACL design. Which of the statements below are true regarding network ACLs? (choose 2)

- With Network ACLs all rules are evaluated until a permit is encountered or continues until the implicit deny
- ✅ Network ACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet

Explanation:-Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny. Network ACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet Network ACL's function at the subnet level, not the instance level With NACLs you can have permit and deny rules All rules are not evaluated before making a decision (security groups do this), they are evaluated in order until a permit or deny is encountered References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- ✅ Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny

Explanation:-Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny. Network ACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet Network ACL's function at the subnet level, not the instance level With NACLs you can have permit and deny rules All rules are not evaluated before making a decision (security groups do this), they are evaluated in order until a permit or deny is encountered References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

- Network ACLs operate at the instance level

Q10)

You created a new Auto Scaling Group (ASG) with two subnets across AZ1 and AZ2 in your VPC. You set the minimum size to 6 instances. After creating the ASG you noticed that all EC2 instances were launched in AZ1 due to limited capacity of the required instance family within AZ2.

You're concerned about the imbalance of resources.

What would be the expected behavior of Auto Scaling once the capacity constraints are resolved in AZ2?

- The ASG will launch three additional EC2 instances in AZ2 and keep the six in AZ1
- The ASG will not do anything until the next scaling event
- The ASG will launch six additional EC2 instances in AZ2
- ✅ The ASG will try to rebalance by first creating three new instances in AZ2 and then terminating three instances in AZ1

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 After launching 3 new instance in AZ2 Auto Scaling will not keep all of the 6 in AZ1, it will terminate 3 of them The ASG will not launch 6 new instances in AZ2 as you only need 6 in total spread (ideally) between both AZs The ASG does not wait for any scaling events, it will automatically perform rebalancing References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

Q11) An EC2 status check on an EBS volume is showing as insufficient-data. What is the most likely explanation?

- ✅ The checks may still be in progress on the volume

Explanation:-The possible values are ok, impaired, warning, or insufficient-data. If all checks pass, the overall status of the volume is ok. If the

check fails, the overall status is impaired. If the status is insufficient-data, then the checks may still be taking place on your volume at the time The checks do not require manual input and they have not failed or the status would be impaired. The volume does not need a certain amount of data on it to be checked properly References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeVolumeStatus.html

- The volume does not have enough data on it to check properly
- The checks have failed on the volume
- The checks require more information to be manually entered

Q12)

You have a three-tier web application running on AWS that utilizes Route 53, ELB, Auto Scaling and RDS. One of the EC2 instances that is registered against the ELB fails a health check.

What actions will the ELB take in this circumstance?

- The ELB will instruct Auto Scaling to terminate the instance and launch a replacement
- The ELB will terminate the instance that failed the health check
- ✅ The ELB will stop sending traffic to the instance that failed the health check

Explanation:-The ELB will simply stop sending traffic to the instance as it has determined it to be unhealthy ELBs are not responsible for terminating EC2 instances. The ELB does not send instructions to the ASG, the ASG has its own health checks and can also use ELB health checks to determine the status of instances ELB does not update Route 53 records References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- The ELB will update Route 53 by removing any references to the instance

---

Q13)

You run a two-tier application with a web tier that is behind an Internet-facing Elastic Load Balancer (ELB). You need to restrict access to the web tier to a specific list of public IP addresses.

What are two possible ways you can implement this requirement? (Choose 2)

- Configure the proxy protocol on the web servers and filter traffic based on IP address
- ✅ Configure the ELB security group to allow traffic only from the specific list of IPs

Explanation:-There are two methods you can use to restrict access from some known IP addresses. You can either use the ELB security group rules or you can configure the ELB to send the X-Forwarded For headers to the web servers. The web servers can then filter traffic using a local firewall such as iptables X-forwarded-for for HTTP/HTTPS carries the source IP/port information. X-forwarded-for only applies to L7. The ELB security group controls the ports and protocols that can reach the front-end listener Proxy protocol applies to layer 4 and is not configured on the web servers A NACL is applied at the subnet level and as they are stateless if you deny all outbound traffic return traffic will be blocked You cannot configure an Internet gateway to allow this traffic. Internet gateways are used for outbound Internet access from public subnets References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- Configure a VPC NACL to allow web traffic from the list of IPs and deny all outbound traffic
- ✅ Configure your ELB to send the X-forwarded for headers and the web servers to filter traffic based on the ELB's "X-forwarded-for" header

Explanation:-There are two methods you can use to restrict access from some known IP addresses. You can either use the ELB security group rules or you can configure the ELB to send the X-Forwarded For headers to the web servers. The web servers can then filter traffic using a local firewall such as iptables X-forwarded-for for HTTP/HTTPS carries the source IP/port information. X-forwarded-for only applies to L7. The ELB security group controls the ports and protocols that can reach the front-end listener Proxy protocol applies to layer 4 and is not configured on the web servers A NACL is applied at the subnet level and as they are stateless if you deny all outbound traffic return traffic will be blocked You cannot configure an Internet gateway to allow this traffic. Internet gateways are used for outbound Internet access from public subnets References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q14)

A membership website your company manages has become quite popular and is gaining members quickly. The website currently runs on EC2 instances with one web server instance and one DB instance running MySQL. You are concerned about the lack of high-availability in the current architecture.

What can you do to easily enable HA without making major changes to the architecture?

- Create a Read Replica in another AZ
- ✅ Install MySQL on an EC2 instance in another AZ and enable replication

Explanation:-If you are installing MySQL on an EC2 instance you cannot enable read replicas or multi-AZ. Instead you would need to use Amazon RDS with a MySQL DB engine to use these features Migrating to RDS would entail a major change to the architecture so is not really feasible. In this example it will therefore be easier to use the native HA features of MySQL rather than to migrate to RDS. You would want to place the second MySQL DB instance in another AZ to enable high availability and fault tolerance References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- Install MySQL on an EC2 instance in the same AZ and enable replication
- Enable Multi-AZ for the MySQL instance

Q15) You have been asked to deploy a new High-Performance Computing (HPC) cluster. You need to create a design for the EC2 instances that ensures close proximity, low latency and high network throughput.Which AWS features will help you to achieve this requirement whilst considering cost? (choose 2)

- ✅ Use EC2 instances with Enhanced Networking

Explanation:-Placement groups are a logical grouping of instances in one of the following configurations: - Cluster—clusters instances into a low-latency group in a single AZ - Spread—spreads instances across underlying hardware (can span AZs) Placement groups are recommended for applications that benefit from low latency and high bandwidth and it s recommended to use an instance type that supports enhanced networking. Instances within a placement group can communicate with each other using private or public IP addresses I/O optimized instances and provisioned IOPS EBS volumes are more geared towards storage performance than network performance Dedicated hosts might ensure close proximity of instances but would not be cost efficient References: https://digitalcloud.training/certification-training/aws-solutions-architect-

associate/compute/amazon-ec2/

- Use Provisioned IOPS EBS volumes
- Use dedicated hosts
- ✅ Use Placement groups

Explanation:-Placement groups are a logical grouping of instances in one of the following configurations: - Cluster—clusters instances into a low-latency group in a single AZ - Spread—spreads instances across underlying hardware (can span AZs) Placement groups are recommended for applications that benefit from low latency and high bandwidth and it s recommended to use an instance type that supports enhanced networking. Instances within a placement group can communicate with each other using private or public IP addresses I/O optimized instances and provisioned IOPS EBS volumes are more geared towards storage performance than network performance Dedicated hosts might ensure close proximity of instances but would not be cost efficient References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

Q16) A Solutions Architect is planning to run some Docker containers on Amazon ECS. The Architect needs to define some parameters for the containers. What application parameters can be defined in an ECS task definition? (choose 2)

- The ELB node to be used to scale the task containers
- ✅ The ports that should be opened on the container instance for your application

Explanation:-Some of the parameters you can specify in a task definition include: Which Docker images to use with the containers in your task How much CPU and memory to use with each container Whether containers are linked together in a task The Docker networking mode to use for the containers in your task What (if any) ports from the container are mapped to the host container instances Whether the task should continue if the container finished or fails The commands the container should run when it is started Environment variables that should be passed to the container when it starts Data volumes that should be used with the containers in the task IAM role the task should use for permissions References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

- The application configuration
- ✅ The container images to use and the repositories in which they are located

Explanation:-Some of the parameters you can specify in a task definition include: Which Docker images to use with the containers in your task How much CPU and memory to use with each container Whether containers are linked together in a task The Docker networking mode to use for the containers in your task What (if any) ports from the container are mapped to the host container instances Whether the task should continue if the container finished or fails The commands the container should run when it is started Environment variables that should be passed to the container when it starts Data volumes that should be used with the containers in the task IAM role the task should use for permissions References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

Q17)

You need to create a file system that can be concurrently accessed by multiple EC2 instances within an AZ. The file system needs to support high throughput and the ability to burst. As the data that will be stored on the file system will be sensitive you need to ensure it is encrypted at rest and in transit.

What storage solution would you implement for the EC2 instances?

- Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes
- Add EBS volumes to each EC2 instance and configure data replication
- Use the Elastic Block Store (EBS) and mount the file system at the block level
- ✅ Use the Elastic File System (EFS) and mount the file system using NFS v4.1

Explanation:-EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud EFS uses the NFSv4.1 protocol Amazon EFS is designed to burst to allow high throughput levels for periods of time EFS offers the ability to encrypt data at rest and in transit References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

Q18) Which service uses a simple text file to model and provision infrastructure resources, in an automated and secure manner?

- OpsWorks
- Simple Workflow Service
- Elastic Beanstalk
- ✅ CloudFormation

Explanation:-AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion. CloudFormation can be used to provision a broad range of AWS resources. Think of CloudFormation as deploying infrastructure as code Elastic Beanstalk is a PaaS solution for deploying and managing applications SWF helps developers build, run, and scale background jobs that have parallel or sequential steps OpsWorks is a configuration management service that provides managed instances of Chef and Puppet References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/

Q19)

An Architect is designing a serverless application that will accept images uploaded by users from around the world. The application will make API calls to back-end services and save the session state data of the user to a database.

Which combination of services would provide a solution that is cost-effective while delivering the least latency?

- API Gateway, Amazon S3, AWS Lambda, DynamoDB
- ✅ Amazon CloudFront, API Gateway, Amazon S3, AWS Lambda, DynamoDB

Explanation:-Amazon CloudFront caches content closer to users at Edge locations around the world. This is the lowest latency option for uploading content. API Gateway and AWS Lambda are present in all options. DynamoDB can be used for storing session state data The option that presents API Gateway first does not offer a front-end for users to upload content to Amazon RDS is not a serverless service so this option can be ruled out Amazon S3 alone will not provide the least latency for users around the world unless you have many buckets in different regions and a way of directing users to the closest bucket (such as Route 3 latency based routing). However, you would then need to manage replicating the data References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/ https://aws.amazon.com/blogs/aws/amazon-cloudfront-content-uploads-post-put-other-methods/

- Amazon S3, API Gateway, AWS Lambda, Amazon RDS

- Amazon CloudFront, API Gateway, Amazon S3, AWS Lambda, Amazon RDS

Q20) You are a Solutions Architect for an insurance company. An application you manage is used to store photos and video files that relate to insurance claims. The application writes data using the iSCSI protocol to a storage array. The array currently holds 10TB of data and is approaching capacity.Your manager has instructed you that he will not approve further capital expenditure for on-premises infrastructure. Therefore, you are planning to migrate data into the cloud. How can you move data into the cloud whilst retaining low-latency access to frequently accessed data on-premise using the iSCSI protocol?

- ✅ Use an AWS Storage Gateway Volume Gateway in cached volume mode

Explanation:-The AWS Storage Gateway service enables hybrid storage between on-premises environments and the AWS Cloud. It provides low-latency performance by caching frequently accessed data on premises, while storing data securely and durably in Amazon cloud storage services AWS Storage Gateway supports three storage interfaces: file, volume, and tape File: - File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3 - File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching -- the question asks for an iSCSI (block) storage solution so a file gateway is not the right solution Volume: - The volume gateway represents the family of gateways that support block-based volumes, previously referred to as gateway-cached and gateway-stored modes - Block storage – iSCSI based – the volume gateway is the correct solution choice as it provides iSCSI (block) storage which is compatible with the existing configuration Tape: - Used for backup with popular backup software - Each gateway is preconfigured with a media changer and tape drives. Supported by NetBackup, Backup Exec, Veeam etc. References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws-storage-gateway/

- Use an AWS Storage Gateway Volume Gateway in stored volume mode
- Use an AWS Storage Gateway Virtual Tape Library
- Use an AWS Storage Gateway File Gateway in cached volume mode

---

Q21)

You are trying to decide on the best data store to use for a new project. The requirements are that the data store is schema-less, supports strongly consistent reads, and stores data in tables, indexed by a primary key.

Which AWS data store would you use?

- ✅ DynamoDB

Explanation:-Amazon Dynamo DB is a fully managed NoSQL (schema-less) database service that provides fast and predictable performance with seamless scalability. Provides two read models: eventually consistent reads (Default) and strongly consistent reads. DynamoDB stores structured data in tables, indexed by a primary key Amazon S3 is an object store and stores data in buckets, not tables Amazon RDS is a relational (has a schema) database service used for transactional purposes Amazon RedShift is a relational (has a schema) database service used for analytics References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

- RDS
- S3
- RedShift

Q22)

Your company has multiple AWS accounts for each environment (Prod, Dev, Test etc.). You would like to copy an EBS snapshot from DEV to PROD. The snapshot is from an EBS volume that was encrypted with a custom key.

What steps do you need to take to share the encrypted EBS snapshot with the Prod account? (choose 2)

- Use CloudHSM to distribute the encryption keys use to encrypt the volume
- ✅ Share the custom key used to encrypt the volume

Explanation:-When an EBS volume is encrypted with a custom key you must share the custom key with the PROD account. You also need to modify the permissions on the snapshot to share it with the PROD account. The PROD account must copy the snapshot before they can then create volumes from the snapshot You cannot share encrypted volumes created using a default CMK key and you cannot change the CMK key that is used to encrypt a volume CloudHSM is used for key management and storage but not distribution You do not need to decrypt the data as there is a workable solution that keeps the data secure at all times References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://aws.amazon.com/blogs/aws/new-cross-account-copying-of-encrypted-ebs-snapshots/

- Create a snapshot of the unencrypted volume and share it with the Prod account
- ✅ Modify the permissions on the encrypted snapshot to share it with the Prod account

Explanation:-When an EBS volume is encrypted with a custom key you must share the custom key with the PROD account. You also need to modify the permissions on the snapshot to share it with the PROD account. The PROD account must copy the snapshot before they can then create volumes from the snapshot You cannot share encrypted volumes created using a default CMK key and you cannot change the CMK key that is used to encrypt a volume CloudHSM is used for key management and storage but not distribution You do not need to decrypt the data as there is a workable solution that keeps the data secure at all times References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/ https://aws.amazon.com/blogs/aws/new-cross-account-copying-of-encrypted-ebs-snapshots/

Q23)

The development team at Digital Cloud Training have created a new web-based application that will soon be launched. The application will utilize 20 EC2 instances for the web front-end. Due to concerns over latency, you will not be using an ELB but still want to load balance incoming connections across multiple EC2 instances. You will be using Route 53 for the DNS service and want to implement health checks to ensure instances are available.

What two Route 53 configuration options are available that could be individually used to ensure connections reach multiple web servers in this configuration? (choose 2)

- ✅ Use Route 53 weighted records and give equal weighting to all 20 EC2 instances

Explanation:-The key requirement here is that you can load balance incoming connections to a series of EC2 instances using Route 53 AND the solution must support health checks. With multi-value answers Route 53 responds with up to eight health records (per query) that are selected at random The weighted record type is similar to simple but you can specify a weight per IP address. You create records that have the same name and type and assign each record a relative weight. In this case you could assign multiple records the same weight and Route 53 will essentially round robin between the records We cannot use the simple record type as it does not support health checks Alias records let you route traffic to selected

AWS resources, such as CloudFront distributions and Amazon S3 buckets. They do not provide equal distribution to multiple endpoints or multi-value answers Failover routing is used for active/passive configurations only References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

✅ Use Route 53 multivalue answers to return up to 8 records with each DNS query

Explanation:-The key requirement here is that you can load balance incoming connections to a series of EC2 instances using Route 53 AND the solution must support health checks. With multi-value answers Route 53 responds with up to eight health records (per query) that are selected at random The weighted record type is similar to simple but you can specify a weight per IP address. You create records that have the same name and type and assign each record a relative weight. In this case you could assign multiple records the same weight and Route 53 will essentially round robin between the records We cannot use the simple record type as it does not support health checks Alias records let you route traffic to selected AWS resources, such as CloudFront distributions and Amazon S3 buckets. They do not provide equal distribution to multiple endpoints or multi-value answers Failover routing is used for active/passive configurations only References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

- Use Route 53 simple load balancing which will return records in a round robin fashion
- Use Route 53 failover routing in an active-active configuration

---

Q24)

A new financial platform has been re-architected to use Docker containers in a micro-services architecture. The new architecture will be implemented on AWS and you have been asked to recommend the solution configuration. For operational reasons, it will be necessary to access the operating system of the instances on which the containers run.

Which solution delivery option will you select?

- ECS with the Fargate launch type
- ECS with a default cluster
- EKS with Kubernetes managed infrastructure
- ✅ ECS with the EC2 launch type

Explanation:-Amazon Elastic Container Service (ECS) is a highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances The EC2 Launch Type allows you to run containers on EC2 instances that you manage so you will be able to access the operating system instances The Fargate Launch Type is a serverless infrastructure managed by AWS so you do not have access to the operating system of the EC2 instances that the container platform runs on The EKS service is a managed Kubernetes service that provides a fully-managed control plane so you would not have access to the EC2 instances that the platform runs on ECS with a default cluster is an incorrect answer, you need to choose the launch type to ensure you get the access required, not the cluster configuration References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

Q25)

A client has made some updates to their web application. The application uses an Auto Scaling Group to maintain a group of several EC2 instances. The application has been modified and a new AMI must be used for launching any new instances.

What do you need to do to add the new AMI?

✅ Create a new launch configuration that uses the AMI and update the ASG to use the new launch configuration

Explanation:-A launch configuration is the template used to create new EC2 instances and includes parameters such as instance family, instance type, AMI, key pair and security groups You cannot edit a launch configuration once defined. In this case you can create a new launch configuration that uses the new AMI and any new instances that are launched by the ASG will use the new AMI Suspending scaling processes 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. It is not useful in this situation A target group is a concept associated with an ELB not Auto Scaling References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

- Modify the existing launch configuration to add the new AMI
- Suspend Auto Scaling and replace the existing AMI
- Create a new target group that uses a new launch configuration with the new AMI

Q26) You have been asked to describe the benefits of using AWS Lambda compared to EC2 instances. Which of the below statements are incorrect?

- With AWS Lambda the customer does not have any responsibility for deploying and managing the compute infrastructure
- AWS Lambda scales automatically
- ✅ With AWS lambda, the client is responsible for launching and administering the underlying AWS compute infrastructure

Explanation:-AWS Lambda lets you run code as functions without provisioning or managing servers. With serverless computing, your application still runs on servers, but all the server management is done by AWS The other statements are correct References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/

- With AWS Lambda you only pay for what you use

Q27)

You are putting together a design for a three-tier web application. The application tier requires a minimum of 6 EC2 instances to be running at all times. You need to provide fault tolerance to ensure that the failure of a single Availability Zone (AZ) will not affect application performance.

Which of the options below is the optimum solution to fulfil these requirements?

- Create an ASG with 6 instances spread across 3 AZs behind an ELB
- Create an ASG with 18 instances spread across 3 AZs behind an ELB
- ✅ Create an ASG with 9 instances spread across 3 AZs behind an ELB

Explanation:-This is simply about numbers. You need 6 EC2 instances to be running even in the case of an AZ failure. The question asks for the “optimum?? solution so you don’t want to over provision. Remember that it takes time for EC2 instances to boot and applications to initialize so it may not be acceptable to have a reduced fleet of instances during this time, therefore you need enough that the minimum number of instances are running without interruption in the event of an AZ outage. References: https://digitalcloud.training/certification-training/aws-solutions-architect-

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

- Create an ASG with 12 instances spread across 4 AZs behind an ELB

Q28)

You need to provide AWS Management Console access to a team of new application developers. The team members who perform the same role are assigned to a Microsoft Active Directory group and you have been asked to use Identity Federation and RBAC.

Which AWS services would you use to configure this access? (choose 2)

- AWS Directory Service Simple AD
- ✅ AWS IAM Roles

Explanation:-AD Connector is a directory gateway for redirecting directory requests to your on-premise Active Directory. AD Connector eliminates the need for directory synchronization and the cost and complexity of hosting a federation infrastructure and connects your existing on-premise AD to AWS. It is the best choice when you want to use an existing Active Directory with AWS services IAM Roles are created and then “assumed?? by trusted entities and define a set of permissions for making AWS service requests. With IAM Roles you can delegate permissions to resources for users and services without using permanent credentials (e.g. user name and password) AWS Directory Service Simple AD is an inexpensive Active Directory-compatible service with common directory features. It is a fully cloud-based solution and does not integrate with an on-premises Active Directory service You map the groups in AD to IAM Roles, not IAM users or groups References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

- AWS IAM Groups
- ✅ AWS Directory Service AD Connector

Explanation:-AD Connector is a directory gateway for redirecting directory requests to your on-premise Active Directory. AD Connector eliminates the need for directory synchronization and the cost and complexity of hosting a federation infrastructure and connects your existing on-premise AD to AWS. It is the best choice when you want to use an existing Active Directory with AWS services IAM Roles are created and then “assumed?? by trusted entities and define a set of permissions for making AWS service requests. With IAM Roles you can delegate permissions to resources for users and services without using permanent credentials (e.g. user name and password) AWS Directory Service Simple AD is an inexpensive Active Directory-compatible service with common directory features. It is a fully cloud-based solution and does not integrate with an on-premises Active Directory service You map the groups in AD to IAM Roles, not IAM users or groups References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/

Q29) Your organization is considering using DynamoDB for a new application that requires elasticity and high-availability. Which of the statements below is true about DynamoDB? (choose 2)

- Data is synchronously replicated across 3 regions
- ✅ Supports cross-region replication which allows you to replicate across regions

Explanation:-DynamoDB uses push button scaling in which you specify the read and write capacity units you need – it does not rely on instance sizes There are limits on the throughput you can provision by default (region specific): US East (N. Virginia) Region: - Per table – 40,000 read capacity units and 40,000 write capacity units - Per account – 80,000 read capacity units and 80,000 write capacity units All Other Regions: - Per table – 10,000 read capacity units and 10,000 write capacity units - Per account – 20,000 read capacity units and 20,000 write capacity unit References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

- ✅ When reading data from Amazon DynamoDB, users can specify whether they want the read to be eventually consistent or strongly consistent

Explanation:-DynamoDB uses push button scaling in which you specify the read and write capacity units you need – it does not rely on instance sizes There are limits on the throughput you can provision by default (region specific): US East (N. Virginia) Region: - Per table – 40,000 read capacity units and 40,000 write capacity units - Per account – 80,000 read capacity units and 80,000 write capacity units All Other Regions: - Per table – 10,000 read capacity units and 10,000 write capacity units - Per account – 20,000 read capacity units and 20,000 write capacity unit References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

- There is no default limit of the throughput you can provision

---

Q30) For which of the following workloads should a Solutions Architect consider using Elastic Beanstalk? (choose 2)

- A data lake
- ✅ A web application using Amazon RDS

Explanation:-A web application using RDS is a good fit as it includes multiple services and Elastic Beanstalk is an orchestration engine A data lake would not be a good fit for Elastic Beanstalk A Long running worker process is a good Elastic Beanstalk use case where it manages an SQS queue - again this is an example of multiple services being orchestrated Content caching would be a good use case for CloudFront A management task run occasionally might be a good fit for AWS Systems Manager Automation References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/ https://aws.amazon.com/elasticbeanstalk/faqs/

- A management task run occasionally
- ✅ A long running worker process

Explanation:-A web application using RDS is a good fit as it includes multiple services and Elastic Beanstalk is an orchestration engine A data lake would not be a good fit for Elastic Beanstalk A Long running worker process is a good Elastic Beanstalk use case where it manages an SQS queue - again this is an example of multiple services being orchestrated Content caching would be a good use case for CloudFront A management task run occasionally might be a good fit for AWS Systems Manager Automation References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-elastic-beanstalk/ https://aws.amazon.com/elasticbeanstalk/faqs/

Q31)

You are working on a database migration plan from an on-premise data center that includes a variety of databases that are being used for diverse purposes. You are trying to map each database to the correct service in AWS.

Which of the below use cases are a good fit for DynamoDB (choose 2)

- ✅ Rapid ingestion of clickstream data

Explanation:-Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability that provides low read and write latency. Because of its performance profile and the fact that it is a NoSQL type of database, DynamoDB is good for rapidly ingesting clickstream data You should use a relational database such as RDS when you need to do complex queries and joins.

Microsoft SQL and Oracle DB are both relational databases so DynamoDB is not a good backup target or migration destination for these types of DB
References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

- Backup for on-premises Oracle DB
- Complex queries and joins
- ✅ Large amounts of dynamic data that require very low latency

Explanation:-Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability that provides low read and write latency. Because of its performance profile and the fact that it is a NoSQL type of database, DynamoDB is good for rapidly ingesting clickstream data You should use a relational database such as RDS when you need to do complex queries and joins. Microsoft SQL and Oracle DB are both relational databases so DynamoDB is not a good backup target or migration destination for these types of DB
References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

Q32)

You are a Solutions Architect at Digital Cloud Training. A client from the agricultural sector has approached you for some advice around the collection of a large volume of data from sensors they have deployed around the country. An application will collect data from over 100,000 sensors and each sensor will send around 1KB of data every minute. The data needs to be stored in a durable, low latency data store. The client also needs historical data that is over 1 year old to be moved into a data warehouse where they can perform analytics using standard SQL queries.

What combination of AWS services would you recommend to the client? (choose 2)

- Elasticache for analytics
- ✅ RedShift for the analytics

Explanation:-The key requirements are that historical data that data is recorded in a low latency, durable data store and then moved into a data warehouse when the data is over 1 year old for historical analytics. This is a good use case for DynamoDB as a data store and RedShift as a data warehouse. Kinesis is used for real-time data, not historical data so is not a good fit Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB provides low read and write latency and is ideal for data ingestion use cases such as this one 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 Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. In this scenario the data being analyzed is not real-time, it is historical Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. We're looking for a data warehouse in this solution so running up EC2 instances may not be cost-effective References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

- Kinesis Data Streams for data ingestion
- ✅ DynamoDB for data ingestion

Explanation:-The key requirements are that historical data that data is recorded in a low latency, durable data store and then moved into a data warehouse when the data is over 1 year old for historical analytics. This is a good use case for DynamoDB as a data store and RedShift as a data warehouse. Kinesis is used for real-time data, not historical data so is not a good fit Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB provides low read and write latency and is ideal for data ingestion use cases such as this one 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 Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. In this scenario the data being analyzed is not real-time, it is historical Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. We're looking for a data warehouse in this solution so running up EC2 instances may not be cost-effective References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

Q33)

You are planning to deploy a number of EC2 instances in your VPC. The EC2 instances will be deployed across several subnets and multiple AZs.

What AWS feature can act as an instance-level firewall to control traffic between your EC2 instances?

- Route table
- Network ACL
- AWS WAF
- ✅ Security Group

Explanation:-Network ACL's function at the subnet level Route tables are not firewalls Security groups act like a firewall at the instance level Specifically, security groups operate at the network interface level AWS WAF is a web application firewall and does not work at the instance level
References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

Q34)

You have been asked to take a snapshot of a non-root EBS volume that contains sensitive corporate data. You need to ensure you can capture all data that has been written to your Amazon EBS volume at the time the snapshot command is issued and are unable to pause any file writes to the volume long enough to take a snapshot.

What is the best way to take a consistent snapshot whilst minimizing application downtime?

- ✅ Un-mount the EBS volume, take the snapshot, then re-mount it again

Explanation:-The key facts here are that whilst minimizing application downtime you need to take a consistent snapshot and are unable to pause writes long enough to do so. Therefore the best option is to unmount the EBS volume and take the snapshot. This will be much faster than shutting down the instance, taking the snapshot, and then starting it back up again Snapshots capture a point-in-time state of an instance and are stored on S3. To take a consistent snapshot writes must be stopped (paused) until the snapshot is complete – if not possible the volume needs to be detached, or if it's an EBS root volume the instance must be stopped If you take the snapshot with the EBS volume attached you may not get a fully consistent snapshot. Though stopping the instance and taking a snapshot will ensure the snapshot if fully consistent the requirement is that you minimize application downtime. You can take snapshots of any EBS volume References: https://digitalcloud.training/certification-training/aws-

solutions-architect-associate/compute/amazon-ebs/

- Take the snapshot while the EBS volume is attached and the instance is running
- Stop the instance and take the snapshot
- You can't take a snapshot for a non-root EBS volume

Q35) You need a service that can provide you with control over which traffic to allow or block to your web applications by defining customizable web security rules. You need to block common attack patterns, such as SQL injection and cross-site scripting, as well as creating custom rules for your own applications.Which AWS service fits these requirements?

- Route 53
- ✅ AWS WAF

Explanation:-AWS WAF is a web application firewall that helps detect and block malicious web requests targeted at your web applications. AWS WAF allows you to create rules that can help protect against common web exploits like SQL injection and cross-site scripting. With AWS WAF you first identify the resource (either an Amazon CloudFront distribution or an Application Load Balancer) that you need to protect. You then deploy the rules and filters that will best protect your applications The other services listed do not enable you to create custom web security rules that can block known malicious attacks References: https://aws.amazon.com/waf/details/

- Security Groups
- CloudFront

Q36) Your company stores important production data on S3 and you have been asked by your manager to ensure that data is protected from accidental deletion. Which of the choices represent the most cost-effective solutions to protect against accidental object deletion for data in an Amazon S3 bucket? (choose 2)

- ✅ Use lifecycle actions to backup the data into Glacier

Explanation:-You must consider multiple facts including cost and the practicality of maintaining a solution. This question has more than two possible solutions so you need to choose the best options from the list. The questions asks for the most cost-effective solution - based on this Glacier and Versioning are the best solutions Glacier can be used to copy or archive files. Glacier integrates with versioning to allow you to choose policies for transitioning current and previous versions to a Glacier archive Versioning stores all versions of an object (including all writes and even if an object is deleted). With versioning you have to pay for the extra consumed space but there are no data egress costs Versioning protects against accidental object/data deletion or overwrites CRR is an Amazon S3 feature that automatically replicates data across AWS Regions. However, there are data egress costs to consider when copying data across regions and you have to pay for 2 copies of the data (vs. a lower cost copy in Glacier) Copying data into an EBS volume would not be cost-effective as it is a higher cost than the other solutions References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- ✅ Enable versioning on the bucket

Explanation:-You must consider multiple facts including cost and the practicality of maintaining a solution. This question has more than two possible solutions so you need to choose the best options from the list. The questions asks for the most cost-effective solution - based on this Glacier and Versioning are the best solutions Glacier can be used to copy or archive files. Glacier integrates with versioning to allow you to choose policies for transitioning current and previous versions to a Glacier archive Versioning stores all versions of an object (including all writes and even if an object is deleted). With versioning you have to pay for the extra consumed space but there are no data egress costs Versioning protects against accidental object/data deletion or overwrites CRR is an Amazon S3 feature that automatically replicates data across AWS Regions. However, there are data egress costs to consider when copying data across regions and you have to pay for 2 copies of the data (vs. a lower cost copy in Glacier) Copying data into an EBS volume would not be cost-effective as it is a higher cost than the other solutions References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Copy your objects to an EBS volume
- You do not need to do anything, by default versioning is enabled

---

Q37) You are designing a solution on AWS that requires a file storage layer that can be shared between multiple EC2 instances. The storage should be highly-available and should scale easily.Which AWS service can be used for this design?

- ✅ Amazon EFS

Explanation:-Amazon Elastic File Service (EFS) allows concurrent access from many EC2 instances and is mounted over NFS which is a file-level protocol An Amazon Elastic Block Store (EBS) volume can only be attached to a single instance and cannot be shared Amazon S3 is an object storage system that is accessed via REST API not file-level protocols. It cannot be attached to EC2 instances An EC2 instance store is an ephemeral storage volume that is local to the server on which the instances runs and is not persistent. It is accessed via block protocols and also cannot be shared between instances References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

- Amazon EC2 instance store
- Amazon S3
- Amazon EBS

Q38)

Your Amazon Virtual Private Cloud (Amazon VPC) includes multiple private subnets. The instances in these private subnets must access third-party payment Application Program Interfaces (APIs) over the Internet.

Which option will provide highly available Internet access to the instances in the private subnets?

- Create a NAT gateway in one Availability Zone and configure your routing to ensure that resources use that NAT gateway in all the Availability Zones.
- Create a customer gateway in each Availability Zone and configure your routing to ensure that resources use the customer gateway in the same Availability Zone.
- ✅ Create a Network Address Translation (NAT) gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

Explanation:-You can use a NAT gateway to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances. If you have resources in multiple Availability Zones and they share one NAT gateway, resources in the other Availability Zones lose Internet access in the event that the NAT gateway's Availability Zone is down. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability zone.

- Create an AWS Storage Gateway in each Availability Zone and configure your routing to ensure that resources use the AWS Storage Gateway in the same Availability Zone.

Q39)

A company runs a service on AWS to provide offsite backups for images on laptops and phones. The solution must support millions of customers, with thousands of images per customer. Images will be retrieved infrequently, but must be available for retrieval immediately.

Which is the MOST cost-effective storage option that meets these requirements?

✔ Amazon S3 Standard-Infrequent Access

Explanation:-Amazon S3 Standard-Infrequent Access is the most cost-effective choice Amazon Glacier with expedited retrievals is fast (1-5 minutes) but not immediate Amazon EFS is a high performance file system and not ideally suited to this scenario, it is also not the most cost-effective option Amazon S3 Standard provides immediate retrieval but is not less cost-effective compared to Standard-Infrequent access References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

- Amazon Glacier with expedited retrievals
- Amazon S3 Standard
- Amazon EFS

Q40) Your Business Intelligence team use SQL tools to analyze data. What would be the best solution for performing queries on structured data that is being received at a high velocity?

- Kinesis Firehose with RDS
- ✔ Kinesis Firehose with RedShift

Explanation:-Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. Firehose Destinations include: Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk 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 EMR is a hosted Hadoop framework and doesn't natively support SQL RDS is a transactional database and is not a supported Kinesis Firehose destination References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

- EMR running Apache Spark
- EMR using Hive

Q41) You are implementing an Elastic Load Balancer (ELB) for an application that will use encrypted communications. Which two types of security policies are supported by the Elastic Load Balancer for SSL negotiations between the ELB and clients? (Choose 2)

✔ Custom security policies

Explanation:-AWS recommend that you always use the default predefined security policy. When choosing a custom security policy you can select the ciphers and protocols (only for CLB) Security groups and network ACLs are security controls that apply to instances and subnets AES 256 is an encryption protocol, not a policy References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- AES 256
- ✔ ELB predefined Security policies

Explanation:-AWS recommend that you always use the default predefined security policy. When choosing a custom security policy you can select the ciphers and protocols (only for CLB) Security groups and network ACLs are security controls that apply to instances and subnets AES 256 is an encryption protocol, not a policy References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

- None of the answers are correct

Q42)

A Solutions Architect is designing a web page for event registrations, and needs a managed service to send a text message to users every time users sign up for an event.

Which AWS service should the Architect use to achieve this?

- AWS Lambda
- ✔ Amazon SNS

Explanation:-Amazon Simple Notification Service (SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud and supports notifications over multiple transports including HTTP/HTTPS, Email/Email-JSON, SQS and SMS Amazon Security Token Service (STS) is used for requesting temporary credentials Amazon Simple Queue Service (SQS) is a message queue used for decoupling application components Lambda is a serverless service that runs code in response to events/triggers References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sns/

- Amazon SQS
- Amazon STS

Q43)

A company are moving to a hybrid cloud model and will be setting up private links between all cloud data centers. An Architect needs to determine the connectivity options available when using AWS Direct Connect and public and private VIFs?

Which options are available to the Architect (choose 2)

✔ Once connected to your VPC through Direct connect you can connect to all AZs within the region

Explanation:-Each AWS Direct Connect connection can be configured with one or more virtual interfaces (VIFs). Public VIFs allow access to public services such as S3, EC2, and DynamoDB. Private VIFs allow access to your VPC. You must use public IP addresses on public VIFs, and private IP addresses on private VIFs Once you have connected to an AWS region using AWS Direct Connect you can connect to all AZs within that region. You can also establish IPSec connections over public VIFs to remote regions. You cannot substitute the Internet connection at the DC with a NAT Gateway -- these are used to allow EC2 instances in private subnets to access the Internet References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/

- You can substitute your internet connection at your DC with AWS's public Internet through the use of a NAT gateway in your VPC
- You can connect to your private VPC subnets over the public VIF
- ✅ You can connect to your private VPC subnets over the private VIF, and to Public AWS services over the public VIF

Explanation:-Each AWS Direct Connect connection can be configured with one or more virtual interfaces (VIFs). Public VIFs allow access to public services such as S3, EC2, and DynamoDB. Private VIFs allow access to your VPC. You must use public IP addresses on public VIFs, and private IP addresses on private VIFs Once you have connected to an AWS region using AWS Direct Connect you can connect to all AZs within that region. You can also establish IPSec connections over public VIFs to remote regions. You cannot substitute the Internet connection at the DC with a NAT Gateway -- these are used to allow EC2 instances in private subnets to access the Internet References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/

Q44)

One of the applications you manage on RDS uses the MySQL DB and has been suffering from performance issues. You would like to setup a reporting process that will perform queries on the database but you're concerned that the extra load will further impact the performance of the DB and may lead to poor customer experience.

What would be the best course of action to take so you can implement the reporting process?

- Configure Multi-AZ to setup a secondary database instance in another Availability Zone
- Configure Multi-AZ to setup a secondary database instance in another region
- ✅ Deploy a Read Replica to setup a secondary read-only database instance

Explanation:-The reporting process will perform queries on the database but not writes. Therefore you can use a read replica which will provide a secondary read-only database and configure the reporting process to use the read replica Read replicas are for workload offloading only and do not provide the ability to write to the database Multi-AZ is used for implementing fault tolerance. With Multi-AZ you can failover to a DB in another AZ within the region in the event of a failure of the primary DB. However, you can only read and write to the primary DB so still need a read replica to offload the reporting job References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- Deploy a Read Replica to setup a secondary read and write database instance

---

Q45)

You have an Amazon RDS Multi-AZ deployment across two availability zones. An outage of the availability zone in which the primary RDS DB instance is running occurs.

What actions will take place in this circumstance? (choose 2)

- ✅ The primary DB instance will switch over automatically to the standby replica

Explanation:-Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it (DR only) A failover may be triggered in the following circumstances: Loss of primary AZ or primary DB instance failure Loss of network connectivity on primary Compute (EC2) unit failure on primary Storage (EBS) unit failure on primary The primary DB instance is changed Patching of the OS on the primary DB instance Manual failover (reboot with failover selected on primary) During failover RDS automatically updates configuration (including DNS endpoint) to use the second node The process to failover is not reliant on network connectivity as it is designed for fault tolerance Connection draining timers are applicable to ELBs not RDS You do not need to manually failover the DB instance, multi-AZ has an automatic process as outlined above References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

- A failover will take place once the connection draining timer has expired
- A manual failover of the DB instance will need to be initiated using Reboot with failover
- ✅ The failover mechanism automatically changes the DNS record of the DB instance to point to the standby DB instance

Explanation:-Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it (DR only) A failover may be triggered in the following circumstances: Loss of primary AZ or primary DB instance failure Loss of network connectivity on primary Compute (EC2) unit failure on primary Storage (EBS) unit failure on primary The primary DB instance is changed Patching of the OS on the primary DB instance Manual failover (reboot with failover selected on primary) During failover RDS automatically updates configuration (including DNS endpoint) to use the second node The process to failover is not reliant on network connectivity as it is designed for fault tolerance Connection draining timers are applicable to ELBs not RDS You do not need to manually failover the DB instance, multi-AZ has an automatic process as outlined above References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

Q46)

A new application you are designing will store data in an Amazon Aurora MySQL DB. You are looking for a way to enable regional disaster recovery capabilities with fast replication and fast failover.

Which of the following options is the BEST solution?

- Create an EBS backup of the Aurora volumes and use cross-region replication to copy the snapshot
- Enable Multi-AZ for the Aurora DB
- Create a cross-region Aurora Read Replica
- ✅ Use Amazon Aurora Global Database

Explanation:-Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages. Aurora Global Database uses storage-based replication with typical latency of less than 1 second, using dedicated infrastructure that leaves your database fully available to serve application workloads. In the unlikely event of a regional degradation or outage, one of the secondary regions can be promoted to full read/write capabilities in less than 1 minute. You can create an Amazon Aurora MySQL DB cluster as a Read Replica in a different AWS Region than the source DB cluster. Taking this approach can improve your disaster recovery capabilities, let you scale read operations into an AWS Region that is closer to your users, and make it easier to migrate from one AWS Region to another. However, this solution would not provide the fast storage replication and fast failover capabilities of the Aurora Global Database and is therefore not the best option Enabling Multi-AZ for the Aurora DB would provide AZ-level resiliency within the region not across regions Though you can take a DB snapshot and replicate it across regions, it does not provide an automated solution and it would not enable fast failover References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/ https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Aurora.Replication.html

---

Q47)

One of your clients is a banking regulator and they run an application that provides auditing information to the general public using AWS Lambda and API Gateway. A Royal Commission has exposed some suspect lending practices and this has been picked up by the media and raised concern amongst the general public. With some major upcoming announcements expected you're concerned about traffic spikes hitting the client's application.

How can you protect the backend systems from traffic spikes?

- Put the APIs in an S3 bucket and publish as a static website using CloudFront
- ✅ Enable throttling limits and result caching in API Gateway

Explanation:-You can throttle and monitor requests to protect your backend. Resiliency through throttling rules is based on the number of requests per second for each HTTP method (GET, PUT). Throttling can be configured at multiple levels including Global and Service Call API Gateway is the front-end component of this application therefore that is where you need to implement the controls. You cannot use CloudFront or ElastiCache to cache APIs. You also cannot put APIs in a bucket and publish as a static website References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

- Use a CloudFront Edge Cache
- Use ElastiCache as the front-end to cache frequent queries

Q48) You need to record connection information from clients using an ELB. When enabling the Proxy Protocol with an ELB to carry connection information from the source requesting the connection, what prerequisites apply? (choose 2)

- ✅ Confirm that your load balancer is not behind a proxy server with Proxy Protocol enabled

Explanation:-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 connections. You need to ensure the client doesn't go through a proxy or there will be multiple proxy headers. You also need to ensure the EC2 instance's TCP stack can process the extra information The back-end and front-end listeners must be configured for TCP HTTPS listeners do not carry proxy protocol information (use the X-Forwarded-For header instead) It doesn't matter what type of pricing model you're using for EC2 (e.g. on-demand, reserved etc.) X-Forwarded-For is a different protocol that operates at layer 7 whereas proxy protocol operates at layer 4 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

- Confirm that your instances are on-demand instances
- ✅ Confirm that your back-end listeners are configured for TCP and front-end listeners are configured for TCP

Explanation:-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 connections. You need to ensure the client doesn't go through a proxy or there will be multiple proxy headers. You also need to ensure the EC2 instance's TCP stack can process the extra information The back-end and front-end listeners must be configured for TCP HTTPS listeners do not carry proxy protocol information (use the X-Forwarded-For header instead) It doesn't matter what type of pricing model you're using for EC2 (e.g. on-demand, reserved etc.) X-Forwarded-For is a different protocol that operates at layer 7 whereas proxy protocol operates at layer 4 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

- Confirm that your load balancer is using HTTPS listeners

Q49)

You need to run a production batch process quickly that will use several EC2 instances. The process cannot be interrupted and must be completed within a short time period.

What is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

- ✅ On-demand instances

Explanation:-The key requirements here are that you need to deploy several EC2 instances quickly to run the batch process and you must ensure that the job completes. The on-demand pricing model is the best for this ad-hoc requirement as though spot pricing may be cheaper you cannot afford to risk that the instances are terminated by AWS when the market price increases Spot instances provide a very low hourly compute cost and are good when you have flexible start and end times. They are often used for use cases such as grid computing and high-performance computing (HPC) 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 There is no such thing as a "flexible instance" References: https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

- Flexible instances
- Spot instances
- Reserved instances
