Answer Sheet

Q1) You were recently promoted to a technical lead role in your DevOps team. Your company has an existing VPC which is quite unutilized for the past few months. The business manager instructed you to integrate your on-premises data center and your VPC. You explained the list of tasks that you'll be doing and mentioned about a Virtual Private Network (VPN) connection. The business manager is not tech-savvy but he is interested to know what a VPN is and its benefits.
What is one of the major advantages of having a VPN in AWS?

- It provides a networking connection between two VPCs which enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.

Explanation:-This option is incorrect because this actually describes VPC Peering and not a VPN connection.

- ✔ It allows you to connect your AWS cloud resources to your on-premises data center using secure and private sessions with IP Security (IPSec) or Transport Layer Security (TLS) tunnels.

Explanation:-Amazon VPC offers you the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network. This option is recommended if you must manage both ends of the VPN connection either for compliance purposes or for leveraging gateway devices that are not currently supported by Amazon VPC's VPN solution. You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a virtual private gateway provides two VPN endpoints (tunnels) for automatic failover. You configure your customer gateway on the remote side of the VPN connection. If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks.
With AWS Site-to-Site VPN, you can connect to an Amazon VPC in the cloud the same way you connect to your branches. AWS Site-to-Site VPN establishes secure and private sessions with IP Security (IPSec) and Transport Layer Security (TLS) tunnels.

- It enables you to establish a private and dedicated network connection between your network and your VPC

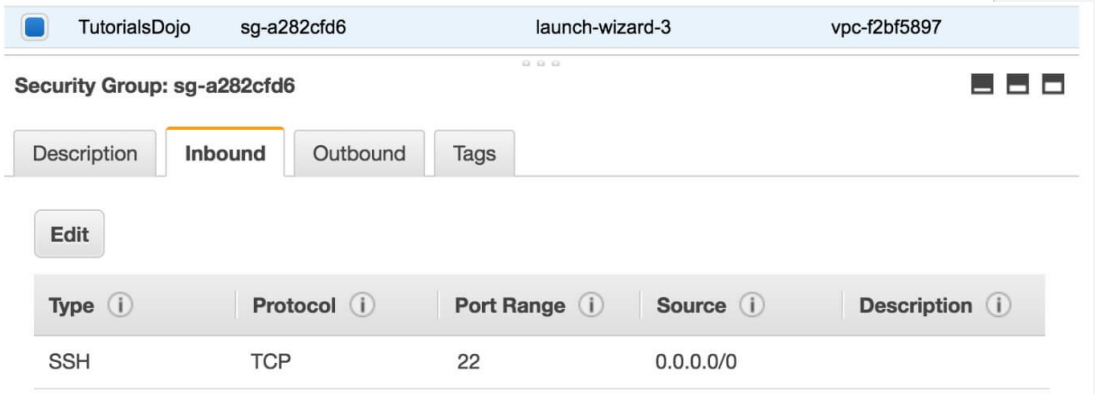
Explanation:-This option is incorrect because this is the advantage of an AWS Direct Connect connection and not a VPN.

- It provides a cost-effective, hybrid connection from your VPC to your on-premises data centers which bypasses the public Internet.

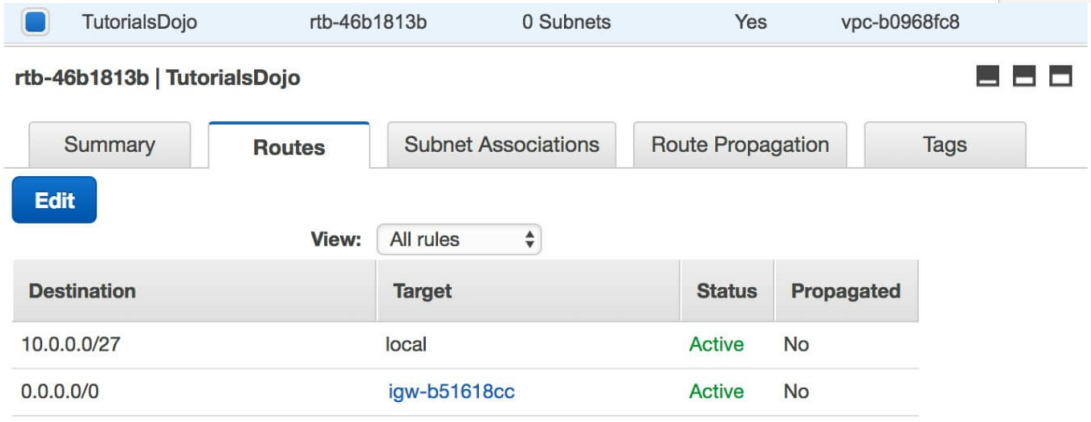
Explanation:-This option is incorrect because although it is true that a VPN provides a cost-effective, hybrid connection from your VPC to your on-premises data centers, it certainly does not bypass the public Internet. A VPN connection actually goes through the public Internet, unlike the AWS Direct Connect connection which has a direct and dedicated connection to your on-premises network.

Q2)

You have an On-Demand EC2 instance located in a subnet in AWS which hosts a web application. The security group attached to this EC2 instance has the following Inbound Rules:



The Route table attached to the VPC is shown below. You can establish an SSH connection into the EC2 instance from the internet. However, you are not able to connect to the web server using your Chrome browser.
Which of the below steps would resolve the issue?



- ✔ In the Security Group, add an Inbound HTTP rule.

Explanation:-The scenario is that you can already connect to the EC2 instance via SSH. This means that there is no problem in the Route Table of your VPC. To fix this issue, you simply need to update your Security Group and add an Inbound rule to allow HTTP traffic.

- In the Route table, add this new route entry: 10.0.0.0/27 -> local
- In the Route table, add this new route entry: 0.0.0.0 -> igw-b51618cc
- In the Security Group, remove the SSH rule.

Q3) A music company is generating confidential data that is saved on their on-premises data center. As a backup solution, the company wants to upload their data on Amazon S3. The company has a policy that any data stored outside its own data center must be encrypted. This way, even if the data is hacked, nobody will be able to read it without the encryption keys.
Which of the following methods can achieve this? (Select TWO.)

- Use SSL to encrypt the data while in transit to Amazon S3.
- Use Amazon S3 bucket policies to restrict access to the data at rest.

✅ Encrypt the data on the client-side using your own master key then upload the data to Amazon S3.

Explanation:-Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3:

Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Use Client-Side Encryption with AWS KMS–Managed Customer Master Key (CMK)

Use Client-Side Encryption Using a Client-Side Master Key

✅ Use Amazon S3 server-side encryption with customer-provided keys.

Explanation:-Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3:

Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Use Client-Side Encryption with AWS KMS–Managed Customer Master Key (CMK)

Use Client-Side Encryption Using a Client-Side Master Key

⚪ Use Amazon S3 server-side encryption with EC2 key pair.

Q4) You are the Solutions Architect for your company's AWS account of approximately 300 IAM users. They have a new company policy that will change the access of 100 of the IAM users to have a particular sort of access to Amazon S3 buckets.
What will you do to avoid the time-consuming task of applying the policy at the individual user?

⚪ Create a new policy and apply it to multiple IAM users using a shell script.

Explanation:-This option is incorrect because you need a new IAM Group for this scenario and not assign a policy to each user via a shell script. This method can save you time but afterwards, it will be difficult to manage all 100 users that are not contained in an IAM Group.

⚪ Create a new IAM role and add each user to the IAM role.

Explanation:-This option is incorrect because you need to use an IAM Group and not an IAM role.

⚪ Create a new S3 bucket access policy with unlimited access for each IAM user.

Explanation:-This option is incorrect because you need a new IAM Group and the method is also time-consuming.

✅ Create a new IAM group and then add the users that require access to the S3 bucket. Afterwards, apply the policy to IAM group.

Explanation:-In this scenario, the best option is to group the set of users in an IAM Group and then apply a policy with the required access to the Amazon S3 bucket. This will enable you to easily add, remove, and manage the users instead of manually adding a policy to each and every 100 IAM users.

Q5) A travel company has a suite of web applications hosted in an Auto Scaling group of On-Demand EC2 instances behind an Application Load Balancer that handles traffic from various web domains such as i-love-manila.com, i-love-boracay.com, i-love-cebu.com and many others. To improve security and lessen the overall cost, you are instructed to secure the system by allowing multiple domains to serve SSL traffic without the need to reauthenticate and reprovision your certificate everytime you add a new domain. This migration from HTTP to HTTPS will help improve their SEO and Google search ranking.
Which of the following is the most cost-effective solution to meet the above requirement?

⚪ Use a wildcard certificate to handle multiple sub-domains and different domains.

⚪ Add a Subject Alternative Name (SAN) for each additional domain to your certificate.

✅ Upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI).

Explanation:-SNI Custom SSL relies on the SNI extension of the Transport Layer Security protocol, which allows multiple domains to serve SSL traffic over the same IP address by including the hostname which the viewers are trying to connect to.

You can host multiple TLS secured applications, each with its own TLS certificate, behind a single load balancer. In order to use SNI, all you need to do is bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client. These features are provided at no additional charge.

To meet the requirements in the scenario, you can upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI).

⚪ Create a new CloudFront web distribution and configure it to serve HTTPS requests using dedicated IP addresses in order to associate your alternate domain names with a dedicated IP address in each CloudFront edge location.

Q6) You are a new Solutions Architect in a large insurance firm. To maintain compliance with HIPAA laws, all data being backed up or stored on Amazon S3 needs to be encrypted at rest. In this scenario, what is the best method of encryption for your data, assuming S3 is being used for storing financial-related data? (Select TWO.)

✅ Encrypt the data using your own encryption keys then copy the data to Amazon S3 over HTTPS endpoints.

Explanation:-Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3.

Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

⚪ Store the data in encrypted EBS snapshots

⚪ Use AWS Shield to protect your data at rest

✅ Enable SSE on an S3 bucket to make use of AES-256 encryption

Explanation:-Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3.

Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

⚪ Store the data on EBS volumes with encryption enabled instead of using Amazon S3

Q7) A company is using multiple AWS accounts that are consolidated using AWS Organizations. They want to copy several S3 objects to another S3 bucket that belonged to a different AWS account which they also own. The Solutions Architect was instructed to set up the necessary permissions for this task and to ensure that the destination account owns the copied objects and not the account it was sent from.
How can the Architect accomplish this requirement?

⚪ Enable the Requester Pays feature in the source S3 bucket. The fees would be waived through Consolidated Billing since both AWS accounts are part of AWS Organizations.

Explanation:-This option is incorrect because the Requester Pays feature is primarily used if you want the requester, instead of the bucket owner, to pay the cost of the data transfer request and download from the S3 bucket. This solution lacks the necessary IAM Permissions to satisfy the requirement. The most suitable solution here is to configure cross-account permissions in S3.

✅ Configure cross-account permissions in S3 by creating an IAM customer managed policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account. Then attach the policy to the IAM user or role that you want to use to copy objects

between accounts.
Explanation:-By default, an S3 object is owned by the account that uploaded the object. That's why granting the destination account the permissions to perform the cross-account copy makes sure that the destination owns the copied objects. You can also change the ownership of an object by changing its access control list (ACL) to bucket-owner-full-control.
However, object ACLs can be difficult to manage for multiple objects, so it's a best practice to grant programmatic cross-account permissions to the destination account. Object ownership is important for managing permissions using a bucket policy. For a bucket policy to apply to an object in the bucket, the object must be owned by the account that owns the bucket. You can also manage object permissions using the object's ACL. However, object ACLs can be difficult to manage for multiple objects, so it's a best practice to use the bucket policy as a centralized method for setting permissions.
To be sure that a destination account owns an S3 object copied from another account, grant the destination account the permissions to perform the cross-account copy. Follow these steps to configure cross-account permissions to copy objects from a source bucket in Account A to a destination bucket in Account B:
- Attach a bucket policy to the source bucket in Account A.
- Attach an AWS Identity and Access Management (IAM) policy to a user or role in Account B.
- Use the IAM user or role in Account B to perform the cross-account copy.

● Set up cross-origin resource sharing (CORS) in S3 by creating a bucket policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account.
Explanation:-This option is incorrect because CORS simply defines a way for client web applications that are loaded in one domain to interact with resources in a different domain, and not on a different AWS account.

● Connect the two S3 buckets from two different AWS accounts to Amazon WorkDocs. Set up cross-account access to integrate the two S3 buckets. Use the Amazon WorkDocs console to copy the objects from one account to the other with modified object ownership assigned to the destination account.
Explanation:-This option is incorrect because Amazon WorkDocs is commonly used to easily collaborate, share content, provide rich feedback, and collaboratively edit documents with other users. There is no direct way for you to integrate WorkDocs and an Amazon S3 bucket owned by a different AWS account. A better solution here is to use cross-account permissions in S3 to meet the requirement.

Q8) You are a new Solutions Architect in your company. Upon checking the existing Inbound Rules of your Network ACL, you saw this configuration:
If a computer with an IP address of 110.238.109.37 sends a request to your VPC, what will happen?

● It will be denied.
● Initially, it will be allowed and then after a while, the connection will be denied.
● Initially, it will be denied and then after a while, the connection will be allowed.
✅ It will be allowed.
Explanation:-Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied immediately regardless of any higher-numbered rule that may contradict it.
We have 3 rules here:
1. Rule 100 permits all traffic from any source.
2. Rule 101 denies all traffic coming from 110.238.109.37
3. The Default Rule (*) denies all traffic from any source.
The Rule 100 will first be evaluated. If there is a match, then it will allow the request. Otherwise, it will then go to Rule 101 to repeat the same process until it goes to the default rule. In this case, when there is a request from 110.238.109.37, it will go through Rule 100 first. As Rule 100 says it will permit all traffic from any source, it will allow this request and will not further evaluate Rule 101 (which denies 110.238.109.37) nor the default rule.

Q9) Your customer has clients all across the globe that access product files stored in several S3 buckets, which are behind each of their own CloudFront web distributions. They currently want to deliver their content to a specific client, and they need to make sure that only that client can access the data. Currently, all of their clients can access their S3 buckets directly using an S3 URL or through their CloudFront distribution. The Solutions Architect must serve the private content via CloudFront only, to secure the distribution of files.
Which combination of actions should you implement to meet the above requirements? (Select TWO.)

● Use S3 pre-signed URLs to ensure that only their client can access the files. Remove permission to use Amazon S3 URLs to read the files for anyone else.
Explanation:-This option is incorrect. Although this could be a valid solution, it doesn't satisfy the requirement to serve the private content via CloudFront only, to secure the distribution of files. A better solution is to set up an origin access identity (OAI) then use Signed URL or Signed Cookies in your CloudFront web distribution.

● Use AWS Cloud Map to ensure that only their client can access the files.
Explanation:-This option is incorrect because AWS Cloud Map is simply a cloud resource discovery service that enables you to name your application resources with custom names and automatically update the locations of your dynamically changing resources.

● Use AWS App Mesh to ensure that only their client can access the files.
Explanation:-This option is incorrect because AWS App Mesh is just a service mesh that provides application-level networking to make it easy for your services to communicate with each other across multiple types of compute infrastructure.

✅ Require the users to access the private content by using special CloudFront signed URLs or signed cookies.
Explanation:-Many companies that distribute content over the Internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee. To securely serve this private content by using CloudFront, you can do the following:
- Require that your users access your private content by using special CloudFront signed URLs or signed cookies.
- Require that your users access your Amazon S3 content by using CloudFront URLs, not Amazon S3 URLs. Requiring CloudFront URLs isn't necessary, but it is recommended to prevent users from bypassing the restrictions that you specify in signed URLs or signed cookies. You can do this by setting up an origin access identity (OAI) for your Amazon S3 bucket. You can also configure the custom headers for a private HTTP server or an Amazon S3 bucket configured as a website endpoint.
All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions. You can generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET. If you are using Microsoft Visual Studio, you can also use AWS Explorer to generate a pre-signed object URL without writing any code. Anyone who receives a valid pre-signed URL can then programmatically upload an object.

✅ Restrict access to files in the origin by creating an origin access identity (OAI) and give it permission to read the files in the bucket.
Explanation:-Many companies that distribute content over the Internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee. To securely serve this private content by using CloudFront, you can do the following:
- Require that your users access your private content by using special CloudFront signed URLs or signed cookies.
- Require that your users access your Amazon S3 content by using CloudFront URLs, not Amazon S3 URLs. Requiring CloudFront URLs isn't necessary, but it is recommended to prevent users from bypassing the restrictions that you specify in signed URLs or signed cookies. You can do this by setting up an origin access identity (OAI) for your Amazon S3 bucket. You can also configure the custom headers for a private HTTP server or an Amazon S3 bucket configured as a website endpoint.
All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions. You can generate a pre-signed URL programmatically using the AWS SDK for Java or the AWS SDK for .NET. If you are using Microsoft Visual Studio, you can also use AWS Explorer to generate a pre-signed object URL without writing any code. Anyone who receives a valid pre-signed URL can then programmatically upload an object.

Q10) You are working for a large financial firm and you are instructed to set up a Linux bastion host. It will allow access to the Amazon EC2 instances running in their VPC. For security purposes, only the clients connecting from the corporate external public IP address 175.45.116.100 should have SSH access to the host.
Which is the best option that can meet the customer's requirement?

● Network ACL Inbound Rule: Protocol – UDP, Port Range – 22, Source 175.45.116.100/32
● Network ACL Inbound Rule: Protocol – TCP, Port Range-22, Source 175.45.116.100/0
✅ Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 175.45.116.100/32
Explanation:-A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.
When setting up a bastion host in AWS, you should only allow the individual IP of the client and not the entire network. Therefore, in the Source, the proper CIDR notation should be used. The /32 denotes one IP address and the /0 refers to the entire network.

● Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 175.45.116.100/32

Q11) You are unable to connect to your newly deployed EC2 instance via SSH from your home computer. However, you were able to

successfully access other existing instances in your VPC without any issues.
Which of the following should you check and possibly correct to restore connectivity?

- Use Amazon Data Lifecycle Manager.

Explanation:-This option is incorrect because this is primarily used to manage the lifecycle of your AWS resources and not to allow certain traffic to go through.

- Configure the Network Access Control List of your VPC to permit ingress traffic over port 22 from your IP.

Explanation:-This option is incorrect because this is not necessary in this scenario as it was specified that you were able to connect to other EC2 instances. In addition, Network ACL is much suitable to control the traffic that goes in and out of your entire VPC and not just on one EC2 instance.

- ✅ Configure the Security Group of the EC2 instance to permit ingress traffic over port 22 from your IP.

Explanation:-When connecting to your EC2 instance via SSH, you need to ensure that port 22 is allowed on the security group of your EC2 instance. A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

- Configure the Security Group of the EC2 instance to permit ingress traffic over port 3389 from your IP.

Explanation:-This option is incorrect because this is relevant to RDP and not SSH.

Q12) You are working for an investment bank as their IT Consultant. You are working with their IT team to handle the launch of their digital wallet system. The applications will run on multiple EBS-backed EC2 instances which will store the logs, transactions, and billing statements of the user in an S3 bucket. Due to tight security and compliance requirements, you are exploring options on how to safely store sensitive data on the EBS volumes and S3.
Which of the below options should be carried out when storing sensitive data on AWS? (Select TWO.)

- ✅ Enable EBS Encryption

Explanation:-Enabling EBS Encryption and enabling Amazon S3 Server-Side or use Client-Side Encryption are correct. Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure.
In Amazon S3, data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options to protect data at rest in Amazon S3.
Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

- Create an EBS Snapshot

Explanation:-This option is incorrect because this is a backup solution of EBS. It does not provide security of data inside EBS volumes when executed.

- ✅ Enable Amazon S3 Server-Side or use Client-Side Encryption

Explanation:-Enabling EBS Encryption and enabling Amazon S3 Server-Side or use Client-Side Encryption are correct. Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure.
In Amazon S3, data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options to protect data at rest in Amazon S3.
Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

- Use AWS Shield and WAF

Explanation:-This option is incorrect because these protect you from common security threats for your web applications. However, what you are trying to achieve is securing and encrypting your data inside EBS and S3.

- Migrate the EC2 instances from the public to private subnet.

Explanation:-This option is incorrect because the data you want to secure are those in EBS volumes and S3 buckets. Moving your EC2 instance to a private subnet involves a different matter of security practice, which does not achieve what you want in this scenario.

Q13) A company needs to launch an Amazon EC2 instance with a persistent block storage to host its application. The stored data must be encrypted at rest.
Which of the following is the most suitable storage solution in this scenario?

- Amazon EC2 Instance Store with SSL encryption.

Explanation:-This option is incorrect because the scenario requires persistent block storage and not temporary storage. Also, enabling SSL is not a requirement in the scenario as it is primarily used to encrypt data in transit.

- ✅ Encrypted Amazon EBS volume using AWS KMS.

Explanation:-Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with EC2 instances. EBS volumes behave like raw, unformatted block devices. You can mount these volumes as devices on your instances. EBS volumes that are attached to an instance are exposed as storage volumes that persist independently from the life of the instance.
Amazon EBS is the persistent block storage volume among the options given. It is mainly used as the root volume to store the operating system of an EC2 instance. To encrypt an EBS volume at rest, you can use AWS KMS customer master keys for the encryption of both the boot and data volumes of an EC2 instance.

- Amazon EBS volume with server-side encryption (SSE) enabled.

Explanation:-This option is incorrect because EBS volumes are only encrypted using AWS KMS. Server-side encryption (SSE) is actually an option for Amazon S3, but not for Amazon EC2.

- Encrypted Amazon EC2 Instance Store using AWS KMS.

Explanation:-This option is incorrect because the scenario requires persistent block storage and not temporary storage. Also, enabling SSL is not a requirement in the scenario as it is primarily used to encrypt data in transit.

Q14) You are working for a startup company that has resources deployed on the AWS Cloud. Your company is now going through a set of scheduled audits by an external auditing firm for compliance.
Which of the following services available in AWS can be utilized to help ensure the right information are present for auditing purposes?

- Amazon VPC

Explanation:-This option is incorrect because a VPC is a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. It does not provide you the auditing information that were asked for in this scenario.

- ✅ AWS CloudTrail

Explanation:-AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.
CloudTrail provides visibility into user activity by recording actions taken on your account. CloudTrail records important information about each action, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. This information helps you to track changes made to your AWS resources and troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.

- Amazon CloudWatch

Explanation:-This option is incorrect because this is a monitoring tool for your AWS resources. Like the above options, it does not provide the needed information to satisfy the requirement in the scenario.

- Amazon EC2

Explanation:-This option is incorrect because EC2 is a service that provides secure, resizable compute capacity in the cloud and does not provide the needed information in this scenario just like the option above.

Q15) A company is using a custom shell script to automate the deployment and management of their EC2 instances. The script is using various AWS CLI commands such as revoke-security-group-ingress, revoke-security-group-egress, run-scheduled-instances and many others.
In the shell script, what does the revoke-security-group-ingress command do?

Removes one or more egress rules from a security group.
Removes one or more security groups from a rule.
Removes one or more security groups from an Amazon EC2 instance.
✓ Removes one or more ingress rules from a security group.

Explanation:-The revoke-security-group-ingress command removes one or more ingress rules from a security group.
Each rule consists of the protocol and the CIDR range or source security group. For the TCP and UDP protocols, you must also specify the destination port or range of ports. For the ICMP protocol, you must also specify the ICMP type and code. If the security group rule has a description, you do not have to specify the description to revoke the rule.
Rule changes are propagated to instances within the security group as quickly as possible. However, a small delay might occur. This example removes TCP port 22 access for the 203.0.113.0/24 address range from the security group named MySecurityGroup. If the command succeeds, no output is returned.
Command:
aws ec2 revoke-security-group-ingress --group-name MySecurityGroup --protocol tcp --port 22 --cidr 203.0.113.0/24

Q16) For data privacy, a healthcare company has been asked to comply with the Health Insurance Portability and Accountability Act (HIPAA). The company stores all its backups on an Amazon S3 bucket. It is required that data stored on the S3 bucket must be encrypted.
What is the best option to do this? (Select TWO.)

Store the data on EBS volumes with encryption enabled instead of using Amazon S3.
Store the data in encrypted EBS snapshots.
✓ Enable Server-Side Encryption on an S3 bucket to make use of AES-256 encryption.

Explanation:-Server-side encryption is about data encryption at restóthat is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a pre-signed URL, that URL works the same way for both encrypted and unencrypted objects.
You have three mutually exclusive options depending on how you choose to manage the encryption keys:
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)
Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

Enable Server-Side Encryption on an S3 bucket to make use of AES-128 encryption.

Explanation:-This option is incorrect as S3 doesn't provide AES-128 encryption, only AES-256.

✓ Before sending the data to Amazon S3 over HTTPS, encrypt the data locally first using your own encryption keys.

Explanation:-Server-side encryption is about data encryption at restóthat is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a pre-signed URL, that URL works the same way for both encrypted and unencrypted objects.
You have three mutually exclusive options depending on how you choose to manage the encryption keys:
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)
Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

Q17) An application is hosted in AWS Fargate and uses RDS database in Multi-AZ Deployments configuration with several Read Replicas. A Solutions Architect was instructed to ensure that all of their database credentials, API keys, and other secrets are encrypted and rotated on a regular basis to improve data security. The application should also use the latest version of the encrypted credentials when connecting to the RDS database.
Which of the following is the MOST appropriate solution to secure the credentials?

Store the database credentials, API keys, and other secrets to AWS ACM.

Explanation:-This option is incorrect because it is just a managed private CA service that helps you easily and securely manage the lifecycle of your private certificates to allow SSL communication to your application. This is not a suitable service to store database or any other confidential credentials.

Store the database credentials, API keys, and other secrets to Systems Manager Parameter Store each with a SecureString data type. The credentials are automatically rotated by default.

Explanation:-This option is incorrect because Systems Manager Parameter Store doesn't rotate its parameters by default.

✓ Use AWS Secrets Manager to store and encrypt the database credentials, API keys, and other secrets. Enable automatic rotation for all of the credentials.

Explanation:-AWS Secrets Manager is an AWS service that makes it easier for you to manage secrets. Secrets can be database credentials, passwords, third-party API keys, and even arbitrary text. You can store and control access to these secrets centrally by using the Secrets Manager console, the Secrets Manager command line interface (CLI), or the Secrets Manager API and SDKs.
In the past, when you created a custom application that retrieves information from a database, you typically had to embed the credentials (the secret) for accessing the database directly in the application. When it came time to rotate the credentials, you had to do much more than just create new credentials. You had to invest time to update the application to use the new credentials. Then you had to distribute the updated application. If you had multiple applications that shared credentials and you missed updating one of them, the application would break. Because of this risk, many customers have chosen not to regularly rotate their credentials, which effectively substitutes one risk for another.
Secrets Manager enables you to replace hardcoded credentials in your code (including passwords), with an API call to Secrets Manager to retrieve the secret programmatically. This helps ensure that the secret can't be compromised by someone examining your code, because the secret simply isn't there. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a schedule that you specify. This enables you to replace long-term secrets with short-term ones, which helps to significantly reduce the risk of compromise.

Store the database credentials, API keys, and other secrets in AWS KMS.

Explanation:-This option is incorrect because this only makes it easy for you to create and manage encryption keys and control the use of encryption across a wide range of AWS services. This is primarily used for encryption and not for hosting your credentials.

Q18) You work for a leading university as an AWS Infrastructure Engineer and also as a professor to aspiring AWS architects. As a way to familiarize your students with AWS, you gave them a project to host their applications to an EC2 instance. One of your students created an instance to host their online enrollment system project but is having a hard time connecting to their newly created EC2 instance. Your students have explored all of the troubleshooting guides by AWS and narrowed it down to login issues.
Which of the following can you use to log into an EC2 instance?

Access Keys
✓ Key Pairs

Explanation:-Amazon EC2 uses publicñkey cryptography to encrypt and decrypt login information. Publicñkey cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair.
To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. On a Linux instance, the public key content is placed in an entry within ~/.ssh/authorized_keys. This is done at boot time and enables you to securely access your instance using the private key instead of a password.

EC2 Connection Strings
Custom EC2 password

Q19) You have two On-Demand EC2 instances inside your Virtual Private Cloud in the same Availability Zone but are deployed to different subnets. One EC2 instance is running a database and the other EC2 instance a web application that connects with the database. You want to ensure that these two instances can communicate with each other for your system to work properly.
What are the things you have to check so that these EC2 instances can communicate inside the VPC? (Select TWO.)

✓ Check if all security groups are set to allow the application host to communicate to the database on the right port and protocol.

Explanation:-First, the Network ACL should be properly set to allow communication between the two subnets. The security group should also be properly configured so that your web server can communicate with the database server

Check if both instances are the same instance class.

Explanation:-This option is incorrect because the EC2 instances do not need to be of the same class in order to communicate with each other.

✓ Check the Network ACL if it allows communication between the two subnets.

Explanation:-First, the Network ACL should be properly set to allow communication between the two subnets. The security group should also be properly configured so that your web server can communicate with the database server.

Check if the default route is set to a NAT instance or Internet Gateway (IGW) for them to communicate.

Explanation:-This option is incorrect because an Internet gateway is primarily used to communicate to the Internet.

Ensure that the EC2 instances are in the same Placement Group.

Explanation:-This option is incorrect because Placement Group is mainly used to provide low-latency network performance necessary for tightly-coupled node-to-node communication.

Q20) A web application, which is used by your clients around the world, is hosted in an Auto Scaling group of EC2 instances behind a Classic Load Balancer. You need to secure your application by allowing multiple domains to serve SSL traffic over the same IP address.
Which of the following should you do to meet the above requirement?

Use Server Name Indication (SNI) on your Classic Load Balancer by adding multiple SSL certificates to allow multiple domains to serve SSL traffic.

Explanation:-This option is incorrect because a Classic Load Balancer does not support Server Name Indication (SNI). You have to use an Application Load Balancer instead or a CloudFront web distribution to allow the SNI feature.

✅ Generate an SSL certificate with AWS Certificate Manager and create a CloudFront web distribution. Associate the certificate with your web distribution and enable the support for Server Name Indication (SNI).

Explanation:-SNI Custom SSL relies on the SNI extension of the Transport Layer Security protocol, which allows multiple domains to serve SSL traffic over the same IP address by including the hostname which the viewers are trying to connect to.

Amazon CloudFront delivers your content from each edge location and offers the same security as the Dedicated IP Custom SSL feature. SNI Custom SSL works with most modern browsers, including Chrome version 6 and later (running on Windows XP and later or OS X 10.5.7 and later), Safari version 3 and later (running on Windows Vista and later or Mac OS X 10.5.6. and later), Firefox 2.0 and later, and Internet Explorer 7 and later (running on Windows Vista and later).

Some users may not be able to access your content because some older browsers do not support SNI and will not be able to establish a connection with CloudFront to load the HTTPS version of your content. If you need to support non-SNI compliant browsers for HTTPS content, it is recommended to use the Dedicated IP Custom SSL feature.

It is not possible to allow multiple domains to serve SSL traffic over the same IP address in AWS

Explanation:-This option is incorrect because AWS does support the use of Server Name Indication (SNI).

Use an Elastic IP and upload multiple 3rd party certificates in your Classic Load Balancer using the AWS Certificate Manager.

Explanation:-This option is incorrect because just like in the above, a Classic Load Balancer does not support Server Name Indication (SNI) and the use of an Elastic IP is not a suitable solution to allow multiple domains to serve SSL traffic. You have to use Server Name Indication (SNI).

Q21)

An online events registration system is hosted in AWS and uses ECS to host its front-end tier and a Multi-AZ RDS for its database tier, which also has a standby replica.

What are the events that will make Amazon RDS automatically perform a failover to the standby replica? (Select TWO.)

Storage failure on secondary DB instance

In the event of Read Replica failure

✅ Loss of availability in primary Availability Zone

Explanation:-Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. Multi-AZ deployments for Oracle, PostgreSQL, MySQL, and MariaDB DB instances use Amazon's failover technology. SQL Server DB instances use SQL Server Database Mirroring (DBM).

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Amazon RDS detects and automatically recovers from the most common failure scenarios for Multi-AZ deployments so that you can resume database operations as quickly as possible without administrative intervention.

The high-availability feature is not a scaling solution for read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a Read Replica.

Amazon RDS automatically performs a failover in the event of any of the following:

Loss of availability in primary Availability Zone

Loss of network connectivity to primary

Compute unit failure on primary

Storage failure on primary

✅ Storage failure on primary

Explanation:-Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. Multi-AZ deployments for Oracle, PostgreSQL, MySQL, and MariaDB DB instances use Amazon's failover technology. SQL Server DB instances use SQL Server Database Mirroring (DBM).

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Amazon RDS detects and automatically recovers from the most common failure scenarios for Multi-AZ deployments so that you can resume database operations as quickly as possible without administrative intervention.

The high-availability feature is not a scaling solution for read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a Read Replica.

Amazon RDS automatically performs a failover in the event of any of the following:

Loss of availability in primary Availability Zone

Loss of network connectivity to primary

Compute unit failure on primary

Storage failure on primary

Compute unit failure on secondary DB instance

Q22)

You are tasked with setting up a Linux bastion host for access to Amazon EC2 instances running in your VPC. Only clients connecting from the corporate external public IP address 72.34.51.100 should have SSH access to the host.

Which option will meet the customer requirement?

✅ Security Group Inbound Rule: Protocol - TCP. Port Range - 22, Source 72.34.51.100/32

Explanation:-Security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level. You must add rules to a security group that enable you to connect to your Linux instance from your IP address using SSH. To add a rule to a security group for inbound SSH traffic using the console In the navigation pane of the Amazon EC2 console, choose Instances. Select your instance and look at the Description tab; Security groups lists the security groups that are associated with the instance. Choose view rules to display a list of the rules that are in effect for the instance. In the navigation pane, choose Security Groups. Select one of the security groups associated with your instance. In the details pane, on the Inbound tab, choose Edit. In the dialog, choose Add Rule, and then choose SSH from the Type list. In the Source field, specify the public IP address of your computer, in CIDR notation. For example, if your IP address is 203.0.113.25, specify 203.0.113.25/32 to list this single IP address in CIDR notation. If your company allocates addresses from a range, specify the entire range, such as 203.0.113.0/24. For information about finding your IP address, see Before You Start. Choose Save.

Security Group Inbound Rule: Protocol - UDP, Port Range - 22, Source 72.34.51.100/32

Network ACL Inbound Rule: Protocol - UDP, Port Range - 22, Source 72.34.51.100/32

Network ACL Inbound Rule: Protocol - TCP, Port Range-22, Source 72.34.51.100/0

Q23) Is decreasing the storage size of a DB Instance permitted?

Depends on the RDMS used

Yes

✅ No

Explanation:-Refer: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html#CHAP_Storage.FactsAbout

---

Q24) You have decided to change the instance type for instances running in your application tier that is using Auto Scaling. In which area below would you change the instance type definition?

- Auto Scaling policy
- Auto Scaling group
- Auto Scaling tags
- ✅ Auto Scaling launch configuration

Explanation:-A launch configuration is a template that an EC2 Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping. If you've launched an EC2 instance before, you specified the same information in order to launch the instance. When you create an EC2 Auto Scaling group, you must specify a launch configuration. You can specify your launch configuration with multiple EC2 Auto Scaling groups. However, you can only specify one launch configuration for an EC2 Auto Scaling group at a time, and you can't modify a launch configuration after you've created it. Therefore, if you want to change the launch configuration for your EC2 Auto Scaling group, you must create a launch configuration and then update your EC2 Auto Scaling group with the new launch configuration. When you change the launch configuration for your EC2 Auto Scaling group, any new instances are launched using the new configuration parameters, but existing instances are not affected. Refer: https://aws.amazon.com/ec2/autoscaling/faqs/

Q25) Fill in the blanks: "To ensure failover capabilities, consider using a _____ for incoming traffic on a network interface".

- primary public IP
- ✅ secondary private IP

Explanation:-To ensure failover capabilities, consider using a secondary private IPv4 for incoming traffic on a network interface. In the event of an instance failure, you can move the interface and/or secondary private IPv4 address to a standby instance. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/scenarios-enis.html

- secondary public IP
- add on secondary IP

Q26) Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

- Use an IAM policy that references the LDAP account identifiers and the AWS credentials.
- ✅ Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP
- Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
- Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.
- Use the LDAP credentials to restrict a group of users from launching specific EC2 instance types.

Q27) What AWS services now support VPC endpoints feature for optimizing security? (Select three)

- ✅ Kinesis

Explanation:-With AWS PrivateLink for Amazon S3, you can provision interface VPC endpoints (interface endpoints) in your virtual private cloud (VPC). These endpoints are directly accessible from applications that are on premises over VPN and AWS Direct Connect, or in a different AWS Region over VPC peering. Interface endpoints are represented by one or more elastic network interfaces (ENIs) that are assigned private IP addresses from subnets in your VPC. Requests that are made to interface endpoints for Amazon S3 are automatically routed to Amazon S3 on the Amazon network. You can also access interface endpoints in your VPC from on-premises applications through AWS Direct Connect or AWS Virtual Private Network (AWS VPN). https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html For security reasons, many AWS customers run their applications within an Amazon Virtual Private Cloud environment (Amazon VPC). With Amazon VPC, you can launch Amazon EC2 instances into a virtual private cloud, which is logically isolated from other networks—including the public internet. With an Amazon VPC, you have control over its IP address range, subnets, routing tables, network gateways, and security settings. To access the public internet, your VPC must have an internet gateway—a virtual router that connects your VPC to the internet. This allows applications running on Amazon EC2 in your VPC to access internet resources, such as Amazon DynamoDB. By default, communications to and from DynamoDB use the HTTPS protocol, which protects network traffic by using SSL/TLS encryption. The following diagram shows how an EC2 instance in a VPC accesses DynamoDB: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html You can use an interface VPC endpoint to keep traffic between your Amazon VPC and Kinesis Data Streams from leaving the Amazon network. Interface VPC endpoints don't require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IPs in your Amazon VPC. https://docs.aws.amazon.com/streams/latest/dev/vpc.html

- DNS Route 53
- ✅ S3

Explanation:-With AWS PrivateLink for Amazon S3, you can provision interface VPC endpoints (interface endpoints) in your virtual private cloud (VPC). These endpoints are directly accessible from applications that are on premises over VPN and AWS Direct Connect, or in a different AWS Region over VPC peering. Interface endpoints are represented by one or more elastic network interfaces (ENIs) that are assigned private IP addresses from subnets in your VPC. Requests that are made to interface endpoints for Amazon S3 are automatically routed to Amazon S3 on the Amazon network. You can also access interface endpoints in your VPC from on-premises applications through AWS Direct Connect or AWS Virtual Private Network (AWS VPN). https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html For security reasons, many AWS customers run their applications within an Amazon Virtual Private Cloud environment (Amazon VPC). With Amazon VPC, you can launch Amazon EC2 instances into a virtual private cloud, which is logically isolated from other networks—including the public internet. With an Amazon VPC, you have control over its IP address range, subnets, routing tables, network gateways, and security settings. To access the public internet, your VPC must have an internet gateway—a virtual router that connects your VPC to the internet. This allows applications running on Amazon EC2 in your VPC to access internet resources, such as Amazon DynamoDB. By default, communications to and from DynamoDB use the HTTPS protocol, which protects network traffic by using SSL/TLS encryption. The following diagram shows how an EC2 instance in a VPC accesses DynamoDB: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html You can use an interface VPC endpoint to keep traffic between your Amazon VPC and Kinesis Data Streams from leaving the Amazon network. Interface VPC endpoints don't require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IPs in your Amazon VPC. https://docs.aws.amazon.com/streams/latest/dev/vpc.html

- ✅ DynamoDB

Explanation:-With AWS PrivateLink for Amazon S3, you can provision interface VPC endpoints (interface endpoints) in your virtual private cloud (VPC). These endpoints are directly accessible from applications that are on premises over VPN and AWS Direct Connect, or in a different AWS Region over VPC peering. Interface endpoints are represented by one or more elastic network interfaces (ENIs) that are assigned private IP addresses from subnets in your VPC. Requests that are made to interface endpoints for Amazon S3 are automatically routed to Amazon S3 on the Amazon network. You can also access interface endpoints in your VPC from on-premises applications through AWS Direct Connect or AWS Virtual Private Network (AWS VPN). https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html For security reasons, many AWS customers run their applications within an Amazon Virtual Private Cloud environment (Amazon VPC). With Amazon VPC, you can launch Amazon EC2 instances into a virtual private cloud, which is logically isolated from other networks—including the public internet. With an Amazon VPC, you have control over its IP address range, subnets, routing tables, network gateways, and security settings. To access the public internet, your VPC must have an internet gateway—a virtual router that connects your VPC to the internet. This allows applications running on Amazon EC2 in your VPC to access internet resources, such as Amazon DynamoDB. By default, communications to and from DynamoDB use the HTTPS protocol, which protects network traffic by using SSL/TLS encryption. The following diagram shows how an EC2 instance in a VPC accesses DynamoDB: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html You can use an interface VPC endpoint to keep traffic between your Amazon VPC and Kinesis Data Streams from leaving the Amazon network. Interface VPC endpoints don't require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IPs in your Amazon VPC. https://docs.aws.amazon.com/streams/latest/dev/vpc.html

- RDS

Q28) What are three characteristics of an Amazon Virtual Private Cloud?

- ✅ Public and private IP addressing

Explanation:-Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications. Refer: https://aws.amazon.com/vpc/

- Broadcasts

- ✅ Multiple private IP addresses per network interface
- Dedicated single tenant hardware only
- ✅ Persistent public IP addresses
- HSRP

Q29) What is the difference between VPC main route table and custom route table?

- VPC does not creates a main route table when started
- Custom route table is the default
- ✅ Custom route table is created for public subnets

Explanation:-The following are the key concepts for route tables.

Main route table—The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.

Custom route table—A route table that you create for your VPC.

Refer: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

- Custom route table is created for private subnets
- Main route table is created for public and private subnets

Q30) What is the purpose of the native VPC router?

- Route packets across the internet
- Route packets between private cloud instances
- ✅ Route packets between subnets

Explanation:-VPC has an implicit router, and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). Link - https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

- Route packets from instances to S3 storage volumes
- Route packets across VPN

Q31) How are private DNS servers assigned to an Amazon VPC?

- Not supported
- ✅ Select nondefault VPC

Explanation:-Refer: https://aws.amazon.com/about-aws/whats-new/2014/11/05/amazon-route-53-now-supports-private-dns-with-amazon-vpc/

- Select default VPC
- Select EC-2 classic

Q32) Which of the following are characteristics of a reserved instance? (Choose 3 answers)

- It can be migrated across Availability Zones
- It is specific to an Amazon Machine Image (AMI)
- ✅ It can be applied to instances launched by Auto Scaling

Explanation:-Refer: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html

- ✅ It is specific to an instance Type

Explanation:-A Reserved Instance has four instance attributes that determine its price - Instance type: For example, m4.large. This is composed of the instance family (for example, m4) and the instance size (for example, large). https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html

- ✅ It can be used to lower Total Cost of Ownership (TCO) of a system

---

Q33) What is an isolated database environment running in the cloud (Amazon RDS) called?

- ✅ DB Instance

Explanation:-A DB instance is an isolated database environment running in the cloud. It is the basic building block of Amazon RDS. A DB instance can contain multiple user-created databases, and can be accessed using the same client tools and applications you might use to access a standalone database instance. Refer: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.DBInstance.html#:~:text=A%20DB%20instance%20is%20an,access%20a%20standalone%20database%20instance.

- DB Unit
- DB Server
- DB Volume

Q34) In regards to IAM you can edit user properties later, but you cannot use the console to change the _____.

- ✅ user name

Explanation:-To change a user's name or path, you must use the AWS CLI, Tools for Windows PowerShell, or AWS API. There is no option in the console to rename a user. Refer: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_manage.html

- password
- default group

Q35) Can I attach more than one policy to a particular entity?

- ✅ Yes always

Explanation:-If you want to define more than one permission for an entity (user or role), you can use multiple statements in a single policy. You can also attach multiple policies. If you try to define multiple permissions in a single statement, your policy might not grant the access that you expect. As a best practice, break up policies by resource type. https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

- Only if within GovCloud
- No
- Only if within VPC

Q36) In AWS, which security aspects are the customer's responsibility? Choose 4 answers

- ✅ Security Group and ACL (Access Control List) settings

Explanation:-The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Refer: https://aws.amazon.com/compliance/shared-responsibility-model/#:~:text=The%20customer%20assumes%20responsibility%20and,AWS%20provided%20security%20group%20firewall.

- Decommissioning storage devices
- ✅ Patch management on the EC2 instance's operating system
- ✅ Life-cycle management of IAM credentials
- Controlling physical access to compute resources
- ✅ Encryption of EBS (Elastic Block Storage) volumes

Q37) Is the SQL Server Audit feature supported in the Amazon RDS SQL Server engine?

- ✅ No

Explanation:-Refer:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html#SQLServer.Concepts.General.FeatureSupport.2012
- Yes

Q38) Which Amazon service can I use to define a virtual network that closely resembles a traditional data center?

- ✅ Amazon VPC

Explanation:-Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS. Refer: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html#:~:text=Amazon%20Virtual%20Private%20Cloud%20(Amazon,the%20scalable%20infrastructure%20of%20AWS.

- Amazon ServiceBus
- Amazon EMR
- Amazon RDS

Q39) It is advised that you watch the Amazon CloudWatch "_____" metric (available via the AWS Management Console or Amazon Cloud Watch APIs) carefully and recreate the Read Replica should it fall behind due to replication errors.

- Write Lag
- Read Replica
- ✅ Replica Lag
- Single Replica

Explanation:-Search Results Featured snippet from the web Amazon RDS allows you to gain visibility into how far a read replica has fallen behind its source DB instance. The number of seconds that the read replica is behind the master is published as an Amazon CloudWatch metric ("Replica Lag") available via the AWS Management Console or Amazon CloudWatch APIs. Refer: https://acloud.guru/forums/aws-certified-sysops-administrator-associate/discussion/-KYSMGj7iTpg-gmqGLDE/what-is-replica-lag#:~:text=Amazon%20RDS%20allows%20you%20to,Console%20or%20Amazon%20CloudWatch%20APIs.

Q40) When using the following AWS services, which should be implemented in multiple Availability Zones for high availability solutions? (Choose 2 answers)

- Amazon DynamoDB
- ✅ Amazon Elastic Compute Cloud (EC2)

Explanation:-Amazon DynamoDB already replicates across AZs, Amazon Simple Notification Service (SNS) and Amazon Simple Storage Service (S3) are a Global Managed Service Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. Refer: https://aws.amazon.com/ec2/

- ✅ Amazon Elastic Load Balancing

Explanation:-Amazon DynamoDB already replicates across AZs, Amazon Simple Notification Service (SNS) and Amazon Simple Storage Service (S3) are a Global Managed Service Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Refer: https://aws.amazon.com/elasticloadbalancing/

- Amazon Simple Notification Service (SNS)
- Amazon Simple Storage Service (S3)

Q41) Your web application front end consists of multiple EC2 instances behind an Elastic Load Balancer. You configured ELB to perform health checks on these EC2 instances, if an instance fails to pass health checks, which statement will be true?

- The instance gets terminated automatically by the ELB.
- The instance gets quarantined by the ELB for root cause analysis.
- The instance is replaced automatically by the ELB.
- ✅ The ELB stops sending traffic to the instance that failed its health check.

Q42) What AWS service automatically publishes access logs every five minutes?

- VPC Flow Logs
- ✅ Elastic Load Balancer

Explanation:-Elastic Load Balancing publishes a log file for each load balancer node every 5 minutes. Log delivery is eventually consistent. The load balancer can deliver multiple logs for the same period. Refer: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html#:~:text=Elastic%20Load%20Balancing%20publishes%20a,logs%20for%20the%20same%20period.

- CloudTrail
- DNS Route 53

Q43)

You have developed a web-based application for file sharing that will allow customers to access files. There are a variety of sizes that include larger .pdf and video files.

What two solution stacks could tenants use for an online file sharing service? (Select two)

- ✅ EC2, ELB, Auto-Scaling, S3
- Route 53, Auto-Scaling, DynamoDB
- EC2, Auto-Scaling, RDS
- ✅ AWS CloudFront

Explanation:-Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. Refer: https://aws.amazon.com/cloudfront/

Q44) What infrastructure services are provided to EC2 instances? (Select three)

- VPN
- ✅ Storage

Explanation:-Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Link - https://aws.amazon.com/types-of-cloud-computing/ When designing your Windows applications to run on Amazon EC2, you can plan for rapid deployment and rapid reduction of compute and storage resources, based on your changing needs. Refer: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/EC2Win_Infrastructure.html

- ✅ Compute
- ✅ Transport
- Security
- Support

Q45) What steps are required from AWS console to copy an EBS-backed AMI for a database instance cross-region?

- Create Snapshot of data volume, select Copy, select destination region
- Select Copy EBS-backed AMI option and destination region
- Select copy database volume and destination region
- ✅ Create Snapshot of EBS-backed AMI, select Copy Snapshot option, select destination region

Explanation:-Search Results Featured snippet from the web Copying an AMI. You can copy an Amazon Machine Image (AMI) within or across AWS Regions using the AWS Management Console, the AWS Command Line Interface or SDKs, or the Amazon EC2 API, all of which support the CopyImage action. You can copy both Amazon EBS-backed AMIs and instance-store-backed AMIs. Refer: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html

- Create Snapshot of Instance-store AMI, select Copy AMI option, select destination region

Q46) How is capacity (compute, storage and network speed) managed and assigned to EC2 instances?

- AMI
- ✓ Instance type

Explanation:-Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more instance sizes, allowing you to scale your resources to the requirements of your target workload. Refer: https://aws.amazon.com/ec2/instance-types/

- IOPS
- Auto-Scaling

Q47) What storage type enable permanent attachment of volumes to EC2 instances?

- S3
- RDS
- TDS
- ✓ EBS

Explanation:-Amazon EBS offers data persistence, dynamic performance adjustments, and the ability to detach and reattach volumes, allowing you to resize clusters for big data analytics engines such as Hadoop and Spark. Refer: https://aws.amazon.com/ebs/?ebs-whats-new.sort-by=item.additionalFields.postDateTime&ebs-whats-new.sort-order=desc

- Instance store

Q48) What is the recommended method for migrating (copying) an EC2 instance to a different region?

- Terminate instance, select region, copy instance to destination region
- ✓ Select AMI associated with EC2 instance and use Copy AMI option

Explanation:-Moving an EC2 Instance to a Different Availability Zone/Region
1. Shutdown / stop the instance.
2. Right-click the instance and select Create
3. Image to make an AMI from the instance.
4. Go to the AMI page, right-click on the new AMI and select Launch Instance.
5. In the new instance settings, choose a specific (different) availability zone.

Refer: https://d1.awsstatic.com/whitepapers/AWS_Migrate_Resources_To_New_Region.pdf

- Stop instance and copy AMI to destination region
- Cross-region copy is not currently supported

Q49) What are two attributes that define an EC2 instance type?

- ✓ vCPU

Explanation:-Refer: https://aws.amazon.com/ec2/instance-types/

- License type
- ✓ EBS volume storage
- IP address
- Auto-Scaling

Q50) For which of the following use cases are Simple Workflow Service (SWF) and Amazon EC2 an appropriate solution? (Choose 2 answers)

- Using as an endpoint to collect thousands of data points per hour from a distributed fleet of sensors
- ✓ Managing a multi-step and multi-decision checkout process of an e-commerce website

Explanation:-Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. The Amazon Simple Workflow Service (Amazon SWF) makes it easy to build applications that coordinate work across distributed components. Amazon SWF gives you full control over implementing tasks and coordinating them without worrying about underlying complexities such as tracking their progress and maintaining their state.

- ✓ Orchestrating the execution of distributed and auditable business processes

Explanation:-Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. The Amazon Simple Workflow Service (Amazon SWF) makes it easy to build applications that coordinate work across distributed components. Amazon SWF gives you full control over implementing tasks and coordinating them without worrying about underlying complexities such as tracking their progress and maintaining their state.

- Using as an SNS (Simple Notification Service) endpoint to trigger execution of video transcoding jobs
- Using as a distributed session store for your web application

Q51) Security groups act like a firewall at the instance level, whereas _____ are an additional layer of security that act at the subnet level.

- DB Security Groups
- VPC Security Groups
- ✓ Network ACLs

Explanation:-A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. Refer: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#:~:text=A%20network%20access%20control%20list,of%20security%20to%20your%20VPC.

Q52)

You launch an Amazon EC2 instance without an assigned AVVS identity and Access Management (IAM) role. Later, you decide that the instance should be running with an IAM role.

Which action must you take in order to have a running Amazon EC2 instance with an IAM role assigned to it?

- Create an image of the instance, and register the image with an IAM role assigned and an Amazon EBS volume mapping.
- Create a new IAM role with the same permissions as an existing IAM role, and assign it to the running instance.
- Create an image of the instance, add a new IAM role with the same permissions as the desired IAM role, and deregister the image with the new role assigned.
- ✓ Create an image of the instance, and use this image to launch a new instance with the desired IAM role assigned.

Explanation:-Link - http://docs.aws.amazon.com/IAM/latest/UserGuide/roles-usingrole-ec2instance.html

Q53) MySQL installations default to port _____.

- ✓ 3306

Explanation:-The default MySQL port number is 3306. Refer: https://aws.amazon.com/getting-started/hands-on/create-mysql-db/

- 443
- 80
- 1158

Q54) What feature requires tenants to disable source/destination check?

- Elastic IP (EIP)
- Data replication
- ✅ VPC peering

Explanation:-If required, update the security group rules that are associated with your instance to ensure that traffic to and from the peer VPC is not restricted. If both VPCs are in the same region, you can reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group rules. Link - https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-basics.html

- NAT

Explanation:-
An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

Refer: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

- Internet gateway

Q55) What's an ECU?

- Extended Cluster User.
- None of these.
- Elastic Computer Usage.
- ✅ Elastic Compute Unit.

Explanation:-Amazon EC2 uses a variety of measures to provide each instance with a consistent and predictable amount of CPU capacity. In order to make it easy for developers to compare CPU capacity between different instance types, we have defined an Amazon EC2 Compute Unit. The amount of CPU that is allocated to a particular instance is expressed in terms of these EC2 Compute Units. We use several benchmarks and tests to manage the consistency and predictability of the performance from an EC2 Compute Unit. The EC2 Compute Unit (ECU) provides the relative measure of the integer processing power of an Amazon EC2 instance. Over time, we may add or substitute measures that go into the definition of an EC2 Compute Unit, if we find metrics that will give you a clearer picture of compute capacity. Refer: https://aws.amazon.com/ec2/faqs/

Q56) In order to optimize performance for a compute cluster that requires low inter-node latency, which of the following feature should you use?

- Multiple Availability Zones
- AWS Direct Connect
- EC2 Dedicated Instances
- ✅ Placement Groups

Explanation:-Cluster – packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications. Refer:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

- VPC private subnets

Q57) What is the default maximum number of MFA devices in use per AWS account (at the root account level)?

- ✅ 1

Explanation:-You can enable only one MFA device per AWS account root user or IAM user. Refer:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable.html#:~:text=You%20can%20enable%20only%20one,root%20user%20or%20IAM%20user.

- 5
- 15
- 10

Q58) What are two primary similarities between AD Connector and Simple AD for cloud directory services?

- ✅ Simple AD requires an on-premises ADS directory

Explanation:-AD Connector simply connects your existing on-premises Active Directory to AWS. AD Connector is your best choice when you want to use your existing on-premises directory with AWS services. Simple AD is an inexpensive Active Directory–compatible service with the common directory features. In most cases, Simple AD is the least expensive option and your best choice if you have 5,000 or fewer users and don't need the more advanced Microsoft Active Directory features. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_best_practices.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

- Simple AD is fully managed and setup in minutes
- ✅ AD Connector requires an on-premises ADS directory

Explanation:-AD Connector simply connects your existing on-premises Active Directory to AWS. AD Connector is your best choice when you want to use your existing on-premises directory with AWS services. Simple AD is an inexpensive Active Directory–compatible service with the common directory features. In most cases, Simple AD is the least expensive option and your best choice if you have 5,000 or fewer users and don't need the more advanced Microsoft Active Directory features. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_best_practices.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

- Simple AD is more scalable than AD Connector
- Simple AD provides enhanced integration with IAM

Q59)

Your team has a tomcat-based Java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC.

Which of the following optimal setup for persistence and security meets the above requirements?

- ✅ Create your RDS instance as part of your Elastic Beanstalk definition and alter its security group to allow access to it from hosts in your application subnets.

Explanation:-Create your RDS instance separately and pass its DNS name to your app's DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself. Refer:
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo.RDS.html

- Create your RDS instance separately and add its IP address to your application's DB connection strings in your code Alter its security group to allow access to it from hosts within your VPC's IP address block.
- Create your RDS instance separately and pass its DNS name to your app's DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself.
- Create your RDS instance separately and pass its DNS name to your's DB connection string as an environment variable Alter its security group to allow access to It from hosts In your application subnets.

Q60)

Your firm has uploaded a large amount of aerial image data to S3 In the past, in your onpremises environment, you used a dedicated group of servers to oaten process this data and used Rabbit MQ - An open source messaging system to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your managertold you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost.

Which of the following option is correct?

- Use SQS for passing job messages use Cloud Watch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.

✅ Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SOS Once data is processed,

Explanation:-Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS Once data is processed, change the storage class of the S3 objects to Glacier.

⚪ Change the storage class of the S3 objects to Reduced Redundancy Storage. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS Once data is processed, change the storage class of the S3 objects to Glacier

⚪ Use SNS to pass job messages use Cloud Watch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.

Q61) Out of the stripping options available for the EBS volumes, which one has the following disadvantage : 'Doubles the amount of I/O required from the instance to EBS compared to RAID 0, because you're mirroring all writes to a pair of volumes, limiting how much you can stripe.' ?

⚪ Raid 0

✅ RAID 1+0 (RAID 10)

Explanation:-RAID 1+0 (RAID 10) doubles the amount of I/O required from the instance to EBS compared to RAID 0, because you're mirroring all writes to a pair of volumes, limiting how much you can stripe. Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

⚪ Raid 1

⚪ Raid

Q62) Where are HTMLfiles sourced from when they are not cached at a CloudFront edge location?

⚪ S3 object

✅ origin HTTP server

Explanation:-CloudFront compares the request with the specifications in your distribution and forwards the request for the files to your origin server for the corresponding file type—for example, to your Amazon S3 bucket for image files and to your HTTP server for HTML files. Refer: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HowCloudFrontWorks.html

⚪ S3 bucket

⚪ Nearest edge location

⚪ RTMP server

⚪ Failover edge location

Q63) What is the capacity of a single Kinesis shard?

⚪ 2000 PUT records per second

⚪ 1 MB/sec data input and 2 MB/sec data output

⚪ 10 MB/sec data input and 10 MB/sec data output

✅ 1000 PUT records per second

Explanation:-Shard is the base throughput unit of a Kinesis stream. One shard can support up to 1000 PUT records per second. Link - https://aws.amazon.com/kinesis/data-streams/faqs/

⚪ Unlimited

Q64) What Amazon AWS service supports real-time processing of data stream from multiple consumers and replay of records?

⚪ DynamoDB

⚪ EMR

✅ Kinesis data streams

Explanation:-Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. Refer: https://aws.amazon.com/kinesis/data-streams/faqs/#:~:text=Amazon%20Kinesis%20Data%20Streams%20enables%20real%2Dtime%20processing%20of%20streaming,to%20multiple%20Amazon%20Kinesis%20Applications.

⚪ SQS

⚪ RedShift

Q65) How is DNS Route 53 configured for Multi-Site fault tolerance? (Select two)

⚪ IP address

✅ Weighted records (non-zero)

Explanation:-Health checks: Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. Each health check that you create can monitor one of the following: The health of a specified resource, such as a web server. The status of other health checks. The status of an Amazon CloudWatch alarm. Additionally, with Amazon Route 53 Application Recovery Controller, you can set up routing control health checks with DNS failover records to manage traffic failover for your application. To learn more, see Amazon Route 53 Application Recovery Controller Developer Guide. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html Weighting fault-tolerant multi-record answers in Amazon Route 53: An Amazon Route 53 weighted record can only be associated with one record, meaning a combination of one name (for example, example.com) and one record type (for example, A). But it is often desirable to weight DNS responses that contain multiple records. For example, you might have eight Amazon EC2 instances or Elastic IP endpoints for a service. If the clients of that service support connection retries (as all common browsers do), then providing multiple IP addresses in DNS responses provides those clients with alternative endpoints in the event of the failure of any particular endpoint. You can even protect against the failure of an availability zone if you configure responses to contain a mix of IPs hosted in two or more availability zones. Multi-record answers are also useful when a large number of clients (for example, mobile web applications) share a small set of DNS caches. In this case, multi-record answers allow clients to direct requests to several endpoints even if they receive a common DNS response from the shared cache. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/TutorialWeightedFTMR.html

✅ Health checks

Explanation:-Health checks: Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. Each health check that you create can monitor one of the following: The health of a specified resource, such as a web server. The status of other health checks. The status of an Amazon CloudWatch alarm. Additionally, with Amazon Route 53 Application Recovery Controller, you can set up routing control health checks with DNS failover records to manage traffic failover for your application. To learn more, see Amazon Route 53 Application Recovery Controller Developer Guide. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html Weighting fault-tolerant multi-record answers in Amazon Route 53: An Amazon Route 53 weighted record can only be associated with one record, meaning a combination of one name (for example, example.com) and one record type (for example, A). But it is often desirable to weight DNS responses that contain multiple records. For example, you might have eight Amazon EC2 instances or Elastic IP endpoints for a service. If the clients of that service support connection retries (as all common browsers do), then providing multiple IP addresses in DNS responses provides those clients with alternative endpoints in the event of the failure of any particular endpoint. You can even protect against the failure of an availability zone if you configure responses to contain a mix of IPs hosted in two or more availability zones. Multi-record answers are also useful when a large number of clients (for example, mobile web applications) share a small set of DNS caches. In this case, multi-record answers allow clients to direct requests to several endpoints even if they receive a common DNS response from the shared cache. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/TutorialWeightedFTMR.html

⚪ Alias records

⚪ Zero weighted records

Q66) What is an Availability Zone?

✅ Data center

Explanation:-AWS Regions are large and widely dispersed into separate geographic locations. Availability Zones are distinct locations within an AWS Region that are engineered to be isolated from failures in other Availability Zones. They provide inexpensive, low-latency network connectivity to other Availability Zones in the same AWS Region. refer - https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/RegionsAndAZs.html

⚪ Multiple VPCs

⚪ Multiple regions

⚪ Single region

⚪ Multiple EC2 server instances

Q67) How are DNS records managed with Amazon AWS to enable high availability?

- Auto-Scaling
- Server health checks
- ✅ Reverse proxy

Explanation:-From split-horizon DNS to customer domain-based DNS records for AWS PrivateLink endpoints, enable varying degrees of traffic rerouting and high availability with ownership/management of the DNS infrastructure. Any implementation must consider a trade-off between service availability, changes to the client application, and management of DNS infrastructure. Refer: https://aws.amazon.com/blogs/apn/reviewing-dns-mechanisms-for-routing-traffic-and-enabling-failover-for-aws-privatelink-deployments/

- Elastic load balancing

Q68) What two statements correctly describe how to add or modify IAM roles to a running EC2 instance?

- ✅ Attach an IAM role to an existing EC2 instance from the EC2 console

Explanation:-Attaching an IAM role to an instance

To attach an IAM role to an instance that has no role, the instance can be in the stopped or running state.

To attach an IAM role to an instance (console)

Open the Amazon EC2 console at https://console.amazonaws.cn/ec2/.

In the navigation pane, choose Instances.

Select the instance, choose Actions, Instance Settings, Attach/Replace IAM role.

Select the IAM role to attach to your instance, and choose Apply.

Refer: https://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

- ✅ Replace an IAM role attached to an existing EC2 instance from the EC2 console

Explanation:-To replace the IAM role on an instance that already has an attached IAM role, the instance must be in the running state. You can do this if you want to change the IAM role for an instance without detaching the existing one first. For example, you can do this to ensure that API actions performed by applications running on the instance are not interrupted.

To replace an IAM role for an instance (console)

Open the Amazon EC2 console at https://console.amazonaws.cn/ec2/.

In the navigation pane, choose Instances.

Select the instance, choose Actions, Instance Settings, Attach/Replace IAM role.

Select the IAM role to attach to your instance, and choose Apply.

Refer: https://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

- Attach an IAM role to the user account and relaunch the EC2 instance
- Add the EC2 instance to a group where the role is a member

Q69) What is the default behavior for an EC2 instance when terminated? (Select two)

- DeleteOnTermination attribute cannot be modified
- EBS root device volume and additional attached volumes are deleted immediately

Explanation:-If EC2 instance is terminated, by default the root volume is also deleted. But the EBS volume attached will be retained. We can change this default behavior by modifying the DeleteOnTermination attribute. When an instance terminates, the data on any instance store volumes associated with that instance is deleted. By default, Amazon EBS root device volumes are automatically deleted when the instance terminates. Refer: When an instance terminates, the data on any instance store volumes associated with that instance is deleted. By default, Amazon EBS root device volumes are automatically deleted when the instance terminates.

- ✅ EBS data volumes that you attach at launch persist
- ✅ EBS root device volume is automatically deleted when instance terminates

---

Q70)

Your company has asked you to capture and forward a real-time data stream on a massive scale directly to RedShift for analysis with BI tools.

What AWS tool is most appropriate that provides the feature set and cost effective?

- DynamoDB
- SQS
- Elastic Map Reduce
- ✅ Kinesis Firehose

Explanation:-With Amazon Kinesis Data Firehose, you pay only for the volume of data you transmit through the service, and if applicable, for data format conversion. You also pay for Amazon VPC delivery and data transfer when applicable. There are no minimum fees or upfront commitments. You don't need staff to operate, scale, and maintain infrastructure or custom applications to capture and load streaming data. https://aws.amazon.com/kinesis/data-firehose/features/ https://aws.amazon.com/kinesis/data-firehose/pricing/

- SNS
- CloudFront

Q71) What feature permits tenants to use a private domain name instead of the domain name that CloudFront assigns to a distribution?

- Route 53
- ✅ CNAME record

Explanation:-In CloudFront, an alternate domain name, also known as a CNAME, lets you use your own domain name (for example, www.example.com) in your files' URLs instead of using the domain name that CloudFront assigns to your distribution. Refer: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/CNAMEs.html#:~:text=In%20CloudFront%2C%20an%20alternate%20domain,CloudFront%20assigns%20to%20your%20distribut

- MX record
- RTMP
- Signed URL

Q72) What Amazon AWS service is available to guarantee the consuming of a unique message only once?

- Beanstalk
- SQL
- Exchange
- ✅ SQS

Explanation:-Standard queues provide at-least-once delivery, which means that each message is delivered at least once. FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it. Refer: https://aws.amazon.com/sqs/faqs/#:~:text=Q%3A%20Does%20Amazon%20SQS%20guarantee,processes%20it%20and%20deletes%20it.

Q73) What is the fastest and easiest method for migrating an on-premises VMware virtual machine to the AWS cloud?

- Amazon Marketplace
- ✅ AWS Server Migration Service

Explanation:- AWS Server Migration Service automates the migration of your on-premises VMware vSphere, Microsoft Hyper-V/SCVMM, and Azure virtual machines to the AWS Cloud. AWS SMS incrementally replicates your server VMs as cloud-hosted Amazon Machine Images (AMIs) ready for deployment on Amazon EC2. Refer: https://docs.aws.amazon.com/server-migration-service/latest/userguide/server-migration.html

- AWS Storage Gateway

- EC2 Import/Export

Q74) Select the stateless protocol from the following?

- FTP
- TCP
- HTTP

Explanation:-HTTP is called as a stateless protocol because each command is request is executed independently, without any knowledge of the requests that were executed before it. It is the protocol used for the web.

- SSH

Q75) What are three valid endpoints for an API gateway?

- RESTful API
- Lambda function

Explanation:-Refer: https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-basic-concept.html

- AWS service
- Web server
- HTTP method

Q76) How is a volume selected (identified) when making an EBS Snapshot?

- account id
- volume id
- tag
- ARN

Explanation:-An Amazon Resource Name (ARN) is a file naming convention used to identify a particular resource in the Amazon Web Services (AWS) public cloud. ARNs, which are specific to AWS, help an administrator track and use AWS items and policies across AWS products and API calls.

Q77) Does Route 53 support MX Records?

- Yes.

Explanation:-Supported DNS record types - Amazon Route 53 Refer: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/ResourceRecordTypes.html#MXFormat

- It supports CNAME records, but not MX records.
- No
- Only Primary MX records. Secondary MX records are not supported.

Q78) If I want my instance to run on a single-tenant hardware, which value do I have to set the instance's tenancy attribute to?

- Dedicated

Explanation:-Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at a hardware level, even if those accounts are linked to a single payer account. However, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances. Refer: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html

- Isolated
- One
- Reserved

Q79) What is the charge for the data transfer incurred in replicating data between your primary and standby?

- No charge. It is free.

Explanation:-You are not charged for the data transfer incurred in replicating data between your primary and standby. Internet data transfer in and out of your DB instance is charged the same as with a standard deployment. Refer: https://aws.amazon.com/rds/faqs/

- Double the standard data transfer charge
- Same as the standard data transfer charge
- Half of the standard data transfer charge

Q80) What are characteristics of Amazon S3? (Choose 2 answers)

- S3 allows you to store objects of virtually unlimited size.
- S3 offers Provisioned IOPS.
- S3 allows you to store unlimited amounts of data.

Explanation:-Amazon S3 has various features you can use to organize and manage your data in ways that support specific use cases, enable cost efficiencies, enforce security, and meet compliance requirements. Data is stored as objects within resources called “buckets”, and a single object can be up to 5 terabytes in size. Refer: https://aws.amazon.com/s3/features/#:~:text=Amazon%20S3%20has%20various%20features,to%205%20terabytes%20in%20size.

- S3 should be used to host a relational database.
- Objects are directly accessible via a URL.

Q81) What is the name of licensing model in which I can use your existing Oracle Database licenses to run Oracle deployments on Amazon RDS?

- Bring Your Own License

Explanation:-Bring Your Own License (BYOL): In this licensing model, you can use your existing Oracle Database licenses to run Oracle deployments on Amazon RDS. To run a DB instance under the BYOL model, you must have the appropriate Oracle Database license (with Software Update License & Support) for the DB instance class and Oracle Database edition you wish to run. You must also follow Oracle's policies for licensing Oracle Database software in the cloud computing environment. DB instances reside in the Amazon EC2 environment, and Oracle's licensing policy for Amazon EC2 is located here. Refer: https://aws.amazon.com/rds/oracle/faqs/

- Role Bases License
- Enterprise License
- License Included

Q82) How can you secure data at rest on an EBS volume?

- Attach the volume to an instance using EC2's SSL interface.
- Write the data randomly instead of sequentially.
- Encrypt the volume using the S3 server-side encryption service.
- Create an IAM policy that restricts read and write access to the volume.
- Use an encrypted file system on top of the EBS volume.

Explanation:-Refer: https://cloudacademy.com/blog/how-to-encrypt-an-ebs-volume-the-new-amazon-ebs-encryption/

Q83) State whether the following statement holds Correct or Incorrect. "The new DB Instance that is created when you promote a Read Replica retains the backup window period."

- CORRECT

Explanation:-The new DB instance that is created when you promote a Read Replica retains the backup retention period, backup window period, and

parameter group of the former Read Replica source When you promote a read replica, the new DB instance that is created retains the option group and the parameter group of the former read replica. The promotion process can take several minutes or longer to complete, depending on the size of the read replica. After you promote the read replica to a new DB instance, it's just like any other DB instance. For example, you can create read replicas from the new DB instance and perform point-in-time restore operations. Because the promoted DB instance is no longer a read replica, you can't use it as a replication target. If a source DB instance has several read replicas, promoting one of the read replicas to a DB instance has no effect on the other replicas. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

- INCORRECT

Q84) Are you able to integrate a multi-factor token service with the AWS Platform?

- Yes, you can integrate private multi-factor token devices to authenticate users to the AWS platform.
- No, you cannot integrate multi-factor token devices with the AWS platform.
- ✅ Yes, using the AWS multi-factor token devices to authenticate users on the AWS platform.

Explanation:-Refer: https://aws.amazon.com/iam/faqs/#MFA_FAQs

---

Q85) Which Amazon Elastic Compute Cloud feature can you query from within the instance to access instance properties?

- Instance user data
- Resource tags
- ✅ Instance metadata

Explanation:-Although you can only access instance metadata and user data from within the instance itself, the data is not protected by authentication or cryptographic methods. Anyone who has direct access to the instance, and potentially any software running on the instance, can view its metadata. Therefore, you should not store sensitive data, such as passwords or long-lived encryption keys, as user data. Refer: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

- Amazon Machine Image

Q86)

A photo-sharing service stores pictures in Amazon Simple Storage Service (S3) and allows application sign-in using an OpenID Connect-compatible identity provider.

Which AWS Security Token Service approach to temporary access should you use for the Amazon S3 operations?

- SAML-based Identity Federation
- Cross-Account Access
- AWS Identity and Access Management roles
- ✅ Web Identity Federation

Explanation:-AWS Identity and Access Management (IAM) supports identity federation, which enables external identities, such as users in your corporate directory, to sign in to the AWS Management Console via single sign-on (SSO). Refer: https://aws.amazon.com/blogs/security/tag/web-identity-federation/

Q87)

You have an application running on an Amazon Elastic Compute Cloud instance, that uploads 5 GB video objects to Amazon Simple Storage Service (S3). Video uploads are taking longer than expected, resulting in poor application performance.

Which method will help improve performance of your application?

- Enable enhanced networking
- ✅ Use Amazon S3 multipart upload

Explanation:-Multipart Upload allows you to upload a single object as a set of parts. After all parts of your object are uploaded, Amazon S3 then presents the data as a single object. With this feature you can create parallel uploads, pause and resume an object upload, and begin uploads before you know the total object size. Refer: https://aws.amazon.com/about-aws/whats-new/2010/11/10/Amazon-S3-Introducing-Multipart-Upload/

- Leveraging Amazon CloudFront, use the HTTP POST method to reduce latency.
- Use Amazon Elastic Block Store Provisioned IOPs and use an Amazon EBS-optimized instance

---

Q88)

You are deploying an application to collect votes for a very popular television show. Millions of users will submit votes using mobile devices. The votes must be collected into a durable, scalable, and highly available data store for real-time public tabulation.

Which service should you use?

- Amazon DynamoDB
- Amazon Redshift
- ✅ Amazon Kinesis

Explanation:-Amazon Kinesis Data Streams is a scalable and durable real-time data streaming service that can continuously capture gigabytes of data per second from hundreds of thousands of sources. Refer: https://aws.amazon.com/kinesis/#:~:text=Amazon%20Kinesis%20Data%20Streams%20is,streams%20into%20AWS%20data%20stores

- Amazon Simple Queue Service

Q89) How does Amazon AWS isolate metrics from different applications for monitoring, store and reporting purposes?

- EC2 instances
- Beanstalk
- CloudTrail
- ✅ namespaces

Explanation:-Container Insights provides automatic dashboards in the CloudWatch console. These dashboards summarize the compute performance, errors, and alarms by cluster, pod/task, and service. For Amazon EKS and k8s, dashboards are also available for nodes/EC2 instances and namespaces. Each dashboard summarizes the list of running pods/tasks or containers by CPU and memory for the selected time window, and allows you to contextually - based on time window and selected pod/task or container - dive deeper into application logs, AWS X-Ray traces, and performance events. You can always retrieve metrics data for any Amazon EC2 instance based on the retention schedules described above. However, the CloudWatch console limits the search of metrics to 2 weeks after a metric is last ingested to ensure that the most up to date instances are shown in your namespace. Refer: https://aws.amazon.com/cloudwatch/features/

- Docker
