Answer Sheet

Q1)

In separate subnets Ryan has launched a couple of EC2 Instances. He is transferring data via the Public IP's of the EC2 Instances. Both Instances are located in the same AZ.

Instances are located in the us-east-1 region. State the data Transfer Charges.

- There are no data transfer charges for instances in the same AZ
- ✅ There will be a data transfer charge of $0.01/GB

Explanation:-The below information is given in the AWS Documentation for data transfer for EC2 Instances Data transferred "in" to and "out" of Amazon EC2, Amazon RDS, Amazon Redshift , Amazon DynamoDB Accelerator (DAX), and Amazon ElastiCache instances or Elastic Network Interfaces across VPC peering connections in the same AWS region is charged at $0.01/GB. Data transferred "in" to and "out" of Amazon Elastic Load Balancing is priced equivalent to Amazon EC2. Data processed by Amazon Elastic Load Balancing

- There are no data transfer charges for instances in the same region
- There is no data transfer charge for the internet

Q2)

To maintain version control and achieve automation for the applications in her organization, Tessy has been requested to use CloudFormation. The environment will consist of several networking components and application services.

State the best possible way to design the template.

- Use CloudFormation custom resources to handle dependencies between stacks
- Create multiple templates in one CloudFormation stack.
- ✅ Create separate templates based on functionality, create nested stacks with CloudFormation.

Explanation:-Create separate stacks templates. So create a separate one for networking so that can be managed separately. Option B is incorrect because custom resources is not the right option for managing multiple components. Option C is incorrect because You can't have multiple templates in one CloudFormation stack Option D is incorrect because maintaining one template can become an issue. For more information on Cloudformation best practises please refer to the below link

- Combine all resources into one template for version control and automation.

Q3)

On an Linux EC2 Instance Riley's team is using a NAT instance.

The Private subnet has a route added for 0.0.0.0/0 for the NAT instance. This NAT instance is being used to download updates from the Internet for instances in the private subnet.

But the IT administrators who are in charge of applying the updates complain of slow response times.

To rectify this issue what can be done? Consider the given Options:

1.) Add another NAT instance. Add another route for 0.0.0.0/0 to the new NAT instance

2.) Replace the NAT instance with a NAT gateway

3.) Upgrade the NAT instance to a larger Instance type

4.) Move the NAT instance to the private subnet to be closer the instances

- Only 2 and 3
- ✅ Only 1 and 4
- Only 1 and 2
- Only 3 and 4

Q4)

Nessy has a team that is trying to ingest 1 TB of data into Amazon S3 using a m4.large instance. Enhanced Networking has been enabled on the instance.

But still the data ingestion process is still running slowly.

State what can be done to rectify the issue.

- Create a VPC endpoint from the instance to S3
- ✅ Consider using 2 m4.large instances and splitting the ingestion of data

Explanation:-Trying to upload a single large object might not be feasible and hence it is better to split the object across multiple instances and carry out the data ingestion process. Option A,B and D are all incorrect since this is a limitation on the instance side

- Use an AWS Direct Connect connection between S3 and the instance
- Create a VPN connection from the instance to S3

Q5)

Parker's current web application is hosted on a set of EC2 Instances which are placed behind an application load balancer. All the Security groups and NACL's have been put into place for tight security.

To ensure blocking of DDos attacks from malicious IP addresses what extra measure can be taken?

- Consider placing an AWS PrivateLink service in front of the Application Load balancer
- Consider placing an AWS Shield service in front of the Application Load balancer

✔ Consider placing the WAF service in front of the Application Load balancer

Explanation:-The AWS Documentation mentions the following AWS WAF is a web application firewall that lets you monitor web requests that are forwarded to Amazon CloudFront distributions or an Application Load Balancer. You can also use AWS WAF to block or allow requests based on conditions that you specify, such as the IP addresses that requests originate from or values in the requests. Option B is incorrect because AWS PrivateLink is used to provide an endpoint for a service Option C is incorrect because A

Consider adding the more restrictive rules to the Network ACL's

---

Q6)

Riley's Company has the following Direct Connect and VPN Connections

Site A - VPN 10.1.0.0/24 AS 65000 65000

Site B - VPN 10.1.0.252/30 AS 65000

Site C - Direct Connect 10.0.0.0/8 AS 65000

Site D - Direct Connect 10.0.0.0/16 AS 65000 65000 65000

You are trying to connect to an IP address of 10.1.0.254.

Out of the following which of the route will be chosen?

Site C

✔ Site B

Explanation:-AWS uses the most specific route in your route table that matches the traffic to determine how to route the traffic (longest prefix match). Hence the one that matches this is Site B. Option A,C and D are all incorrect since the shortest prefix would be chosen.

Site A

Site D

Q7)

Robert is IT Manager at TPT Limited and has configured a hosted zone in Route 53.

How will Robert be able to see the types of records being requested to the zone?

Configure Cloud trail

Configure VPC Flow Logs

Configure Cloud watch metrics

None of these

✔ Configure Amazon Route 53 logging

Q8)

Data streams from thousands of devices is been received by your Amazon Kinesis application. The data is then stored in an on-premises Hadoop cluster. Now you are concerned about historical data that shows periods of sustained traffic between 1 Gbps and 2 Gbps during peaks. Amazon Kinesis and your data center have a secure, faulttolerant connectivity must be ensured by you.

To address these needs what should be implemented by you?

Deploy two 1-Gbps Direct Connect connections.

✔ Deploy three 1-Gbps Direct Connect connections.

Deploy a single 1-Gbps Direct Connect connection with a VPN backup.

Set up an IPsec VPN connection over Direct Connect with two tunnels.

Q9)

Stella has a web application (app.mycompany.com) running on an EC2 instance with a single elastic network interface in a subnet in a VPC. Because of a network redesign, she needs to move the web application to a different subnet in the same Availability Zone.

Out of the following migration strategies which meet the requirements?

Make an API call to change the subnet association of the elastic network interface.

✔ Launch a new instance in the subnet via an AMI created from the instance, and redirect new connections to this new instance using DNS. Decommission the old instance.

Create an elastic network interface in the new subnet. Attach this interface to the instance, and detach the old interface.

Change the IP addresses manually to another subnet within the server operating system.

Q10)

For PCI compliance you are architecting your e-business application. You need to monitor web application logs to identify any malicious activity to meet the compliance requirements.

To change the network interface of web instances you also need to monitor for remote attempts.

To achieve this goal which two AWS services will be helpful?

AWS CloudTrail and VPC Flow Logs

Amazon CloudWatch Logs and VPC Flow Logs

✔ AWS CloudTrail and CloudWatch Logs

AWS CloudTrail and AWS Config

Q11)

Confidential data is being processed by an application that Annie has. The data is currently stored in her data center.

She is moving workloads to AWS, and she needs to ensure confidentiality and integrity of the data in transit to her VPC.

Her company has an existing AWS Direct Connect connection.

To set up the most cost-effective connection between her on-premises data center and AWS what combination of steps should Annie perform?

1.) Set up a VPC with a virtual private gateway.

2.) Set up a VPC with an Internet gateway.

3.) Configure a public virtual interface on your Direct Connect connection.

4.) Configure a private virtual interface to the virtual private gateway.

5.) Set up an IPsec tunnel between your customer gateway appliance and the virtual private gateway.

- ✅ Only 1, 3 and 5
- Only 1, 3 and 4
- Only 4 and 5
- Only 2, 4 and 5

Q12)

With a clientside, smartcard-stored certificate you are deploying a web application in a VPC that requires SSL mutual authentication. The ELB Classic Load Balancer listener must support mutual authentication between the client and the application.

For this application which loads balancer protocol should you select?

- SSL
- HTTPS
- HTTP
- ✅ TCP

Q13)

An HPC solution is been architected in AWS. The system consists of a cluster of EC2 instances that require low-latency communications between them.

To meet these requirements which method should you use to set up a cluster?

- Choose an EC2 instance type that offers enhanced networking. Attach a 10-Gbps non-blocking elastic network interface to the instances. Configure the elastic network interface to optimize network performance to reduce latency.
- ✅ Create a placement group. Choose an EC2 instance type compatible with placement groups for the cluster. Launch instances for the cluster in the placement group.
- Launch Amazon EC2 instances with the largest available number of cores and RAM. Attach all instances to an Amazon EBS PIOPS volume. Implement a shared memory system across all instances in the cluster, using this shared EBS volume to minimize latency of communication.
- Create a VPC with one subnet in a single Availability Zone. Keep the size of the subnet equal to the number of instances required in the cluster. Launch instances for the cluster in this small subnet to guarantee low-latency network performance.

Q14)

Robert is system administrator at TPT Limited and has a VPN connection between on-premise and an AWS VPC. Robert is responsible to ensure instances in the VPC reach the Internet and for which an Internet gateway has been attached.

How route tables be configured by Robert so that traffic can flow through the VPN and the Internet?

- Setup one route table. Add one route of 0.0.0.0/0 to the Internet and another route of 0.0.0.0/0 route for the Virtual Private gateway. Attach the Route table to the subnets In the VPC.
- Setup 2 Route tables. One route table with a default route to the Internet and another one with the default route to the Virtual Private gateway. Attach the Route tables to the sub nets In the VPC.
- ✅ Setup one route table. Add one route of 0.0.0.0/0 to the Internet and one specific prefix route for the Virtual Private gateway. Attach the Route table to the subnets in the VPC.
- Setup 2 Route tables. One route table with a default route to the Internet and another one with the s prefix route to the Virtual Private gateway. Attach the Route tables to the subnets in the VPC.
- None of these

Q15)

On a set of EC2 Instances a Company 'PNX.co' is Planning on hosting an application.

To ensure that the application is (HIPAA) compliant there is a requirement for complete end to end encryption for the data. How can Riley achieve this?

- Ensure that the traffic is encrypted using KMS
- Setup a VPN connection between the EC2 Instance and the Internet
- Setup a Direct Connect connection between the EC2 Instance and the Internet
- ✅ Use SSL to encrypt all the data at the application layer

Explanation:-Since the data needs to be encrypted end to end, use an SSL certificate which can be mapped to the application. Option A is incorrect

because this can be used to encrypt data at rest Option B is incorrect because this will not encrypt traffic end to end Option C is incorrect because this is not a feasible option for this scenario

---

Q16)

For managing Blue Green deployments Ted's company is currently planning on using Route53. They have already setup an 80%-20% for a new deployment.

How can Ted ensure to stop sending traffic to the older setup once all testing is complete?

- Delete the weighted resource record
- Change the resource record to a simple routing policy
- Change the resource record weight to 100
- ✅ Change the resource record weight to 0

Explanation:-The AWS Documentation mentions the following to support this answer Enter an integer between 0 and 255. To disable routing to a resource, set Weight to 0. If you set Weight to 0 for all of the records in the group, traffic is routed to all resources with equal probability. This ensures that you don't accidentally disable routing for a group of weighted records. Options A and B are incorrect since you need to first mark the resource record as 0 Option C is incorrect because this will cause the

---

Q17)

In an AWS VPC Parker has a set of instances setup. He needs to ensure that instances in the VPC receive host names from the AWS DNS. He has set the enableDnsHostname attribute set to true for his VPC.

But stille the instances are still not receiving the host names when they are being launched.

State the underlying issue of the following.

- ✅ The enableDnsSupport is not set to true for the VPC
- You need to configure a Route 53 private hosted zone first
- The Auto-Assign Public IP is not set for the Subnet in which the Instance is launched The Auto-Assign Public IP is not set for the Subnet in which the Instance is launched
- You need to configure a Route 53 public hosted zone first

Q18) In AWS Natallie has setup a Cloudfront distribution. She wants to use the AWS Certification Manager along with Cloudfront. She is setting up Cloudfront, but she cannot see the ACM certificate that she has created at an earlier stage to associate with the distribution. _____ Could be the underlying issue.

- Natallie need to ensure that an alias record is created in Route 53 first
- Natallie need to ensure that a CNAME record is created in Route 53 first
- Natallie need to upload the certificate directly to Cloudfront after the distribution is created
- ✅ Natallie has not uploaded or created the certificate in the right region

---

Q19)

TPT Limited wants to create a VPC endpoint for their SaaS product hosted in AWS. TPT Limited wants give this link to their customer who will access from their application working on UDP.

TPT Limited is planning to provide a DNS name for the link to the customer but, customer complains of not being able to use the link from within their application. Identify the reason for this behaviour.

- The gateway endpoint has a policy that denies access. This should be modified accordingly.
- The customer needs to use a NAT device to access the endpoint service
- ✅ The service endpoint only works on the TCP protocol
- The customer needs to create a Network load balancer to access the endpoint service
- None of these

Q20)

TPT Limited has multiple remote branch offices which are to be connected with AWS VPC.

Which of the following will accomplish the task easily?

- AWS Direct Connect with a Private VIF
- AWS Direct Connect with a Public V1F
- VPC Peering
- ✅ VPN Cloud hub
- None of these

Q21)

TPT Limited has just configured a private hosted zone in Route 53 and a VPN connection between the AWS VPC and on-premise network.

Which of the following will resolve DNS names from on-premise to the resources records defined in the Private hosted zone?

- Configure a DNS resolver in the VPC which will resolve DNS requests to the Route 53 private hosted zone.
- Create a DNS forwarder server in your on-premise location. Configure the VPC with a new DHCP options s which uses this DNS forwarder.
- ✅ Configure a DNS forwarder In the VPC which will forward DNS requests to the Route 53 private hosted zone
- Create a DNS resolver server in your on-premise location. Configure the VPC with a new DHCP options set which uses this DNS resolver.

- None of these

Q22)

TPT Limited is hosting an application of a NGINX web server which is hosted behind a load balancer.

How would TPT Limited ensure restricted access to certain locations for the content hosted on the Web server?

- ✓ Use the IP addresses in the X-Forwarded-For HTTP header and then restrict content via Cloud front geo-restrictions.
- Use the ELB itself to restrict content via geo-restrictions
- Use the ELB logs to create a blacklist for restrictions
- Use the NGINX logs to get the web server variable and then use the IP address to restrict content via Cloud front geo-restrictions.
- None of these

Q23)

TPT Limited is using the Net Flow software for monitoring and accessing details of traffic flows between systems in their On-premise network.

Which of the following will provide the same functionality if TPT Limited migrates to AWS?

- AWS Cloudwatch logs
- AWS Config
- AWS Cloudwatch metrics
- ✓ AWS VPC Flow Logs
- None of these