Answer Sheet

Q1)

A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket.

Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?

✓ Access the S3 bucket through a VPC endpoint for S3
● Access the S3 bucket through a NAT gateway.
● Access the S3 bucket through a proxy server
● Access the S3 bucket through the SSL protected S3 endpoint (Incorrect)

Q2)

Your company has confidential documents stored in the simple storage service.

Due to compliance requirements, you have to ensure that the data in the S3 bucket is available in a different geographical location.

As an architect what is the change you would make to comply with this requirement.

● Create a snapshot of the S3 bucket and copy it to another region
● Copy the data to an EBS Volume in another Region
● Apply Multi-AZ for the underlying S3 bucket
✓ Enable Cross region replication for the S3 bucket

Q3)

When managing permissions for the API gateway, what can be used to ensure that the right level of permissions are given to developers, IT admins and users?

These permissions should be easily managed.

● Use IAM Access Keys to create sets of keys for the different types of users.
● Use the AWS Config tool to manage the permissions for the different users
✓ Use IAM Policies to create different policies for the different types of users.
● Use the secure token service to manage the permissions for the different users

Q4)

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance.

A Linux bastion host is used to apply schema updates to the database – administrators connect to the host via SSH from a corporate workstation.

The following security groups are applied to the infrastructure-

• sgLB – associated with the ELB

• sgWeb – associated with the EC2 instances.

• sgDB – associated with the database

• sgBastion – associated with the bastion host Which security group configuration will allow the application to be secure and functional?

✓ sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range
● sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range
● sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLB sgBastion: allow port 22 traffic from the VPC IP address range
● sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range

Q5)

An application running on EC2 instances in a VPC must access sensitive data in the data center. The access must be encrypted in transit and have consistent low latency.

Which hybrid architecture will meet these requirements?

● A VPN between the VPC and the data center.
✓ A VPN between the VPC and the data center over a Direct Connect connection
● Expose the data with a public HTTPS endpoint.
● A Direct Connect connection between the VPC and data center. (Incorrect)

Q6)

Your application currently uses customer keys which are generated via AWS KMS in the US east region.

You now want to use the same set of keys from the EU-Central region.

How can this be accomplished?

- ● Use the backing key from the US east region and use it in the EU-Central region
- ● Use key rotation and rotate the existing keys to the EU-Central region
- ● Export the key from the US east region and import them into the EU-Central region
- ✓ This is not possible since keys from KMS are region specific

Q7)

You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet.

This instance needs to connect to an EC2 Instance that will host an Oracle database.

Which of the following steps should be followed to ensure a secure setup is in place

- ✓ Create a database security group and ensure the web security group to allowed incoming access
- ✓ Place the EC2 Instance with the Oracle database in a separate private subnet
- ● Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication.
- ● Ensure the database security group allows incoming traffic from 0.0.0.0/0

Q8)

A company is using a Redshift cluster to store their data warehouse.

There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database.

How can this be achieved?

- ● Use SSL/TLS for encrypting the data
- ✓ Use AWS KMS Customer Default master key
- ● Encrypt the EBS volumes of the underlying EC2 Instances
- ● Use S3 Encryption

Q9)

A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions.

The audit needs to be applied for future regions as well. Which of the following can be used to fulfil this requirement.

- ● Create a Cloudtrail for each region. Use Cloudformation to enable the trail for all future regions.
- ✓ Ensure one Cloudtrail trail is enabled for all regions.
- ● Ensure Cloudtrail for each region. Then enable for each future region.
- ● Create a Cloudtrail for each region. Use AWS Config to enable the trail for all future regions.

Q10)

A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists.

They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.

- ● Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation
- ✓ Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
- ● Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
- ● Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation

Q11)

A company is planning to run a number of Admin related scripts using the AWS Lambda service. There is a need to understand if there are any errors encountered when the script run.

How can this be accomplished in the most effective manner.

- ● Use the AWS Config service to monitor for errors
- ● Use Cloudtrail to monitor for errors
- ✓ Use Cloudwatch metrics and logs to watch for errors
- ● Use the AWS Inspector service to monitor for errors

Q12)

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity.

Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below

- ● Amazon AWS Config
- ● Amazon VPC Flow Logs

✓ Amazon Cloudwatch Logs
✓ Amazon Cloudtrail

Q13)

Your company currently has a set of EC2 Instances hosted in a VPC. The IT Security department is suspecting a possible DDos attack on the instances.

What can you do to zero in on the IP addresses which are receiving a flurry of requests.

● Use AWS Trusted Advisor to get the IP addresses accessing the EC2 Instances
● Use AWS Config to get the IP addresses accessing the EC2 Instances
● Use AWS Cloud trail to get the IP addresses accessing the EC2 Instances
✓ Use VPC Flow logs to get the IP addresses accessing the EC2 Instances

Q14)

You have a set of application , database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly.

There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take

● Check the Outbound security rules for the database security group Check the both the Inbound and Outbound security rules for the application security group
● Check the both the Inbound and Outbound security rules for the database security group Check the Inbound security rules for the application security group
● Check the Outbound security rules for the database security group Check the Inbound security rules for the application security group
✓ Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group

Q15)

A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum.

Which of the following would help fulfill this requirement? Choose 2 answers from the options given below

● AWS NAT gateways
● AWS VPC Peering
✓ AWS VPN
✓ AWS Direct Connect

Q16) TPT Limited wants to use their own managed DNS instance for routing DNS requests. What will ensure that instance in a VPC does not use AWS DNS for routing DNS requests?

● Change the subnet configuration to allow DNS requests from the new DNS Server
✓ Create a new DHCP options set and replace the existing one.
● None of these
● Change the route table for the VPC
● Change the existing DHCP options set

Q17)

A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working.

What is the other step that needs to be followed to ensure that the AD domain join can work as intended?

✓ Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets
● Change the VPC peering connection to a Direct Connect connection
● Change the VPC peering connection to a VPN connection
● Ensure that the AD is placed in a public subnet

Q18) Which of the following will address the requirement at TPT Limited, for storing objects in an Amazon S3 bucket with a key which is automatically managed and rotated?

● AWS Customer Keys
● AWS Cloud HSM
● None of these
✓ AWS S3 Server side encryption
● AWS KMS

Q19)

A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition , it should be ensured that objects are available in a secondary region if the primary one goes down.

Which of the following can help fulfill these requirements? Choose 2 answers from the options given below

● Enable the Bucket ACL and add a condition for { "Null": { "aws:MultiFactorAuthAge": true }}
✓ For the Bucket policy add a condition for { "Null": { "aws:MultiFactorAuthAge": true }}
✓ Enable bucket versioning and also enable CRR
● Enable bucket versioning and enable Master Pays

Q20) Robert is working as an administrator at TPT Limited has been asked to inspect the running processes on an EC2 instance to inspect for security issue. Which of the following is the best way to meet the requirement without interfering the continuous running of the instance?

✓ Use the SSM Run command to send the list of running processes information to an S3 bucket.
● Use AWS Config to see the changed process information on the server
● Use AWS Cloudwatch to record the processes running on the server
● None of these
● Use AWS Cloudtrail to record the processes running on the server to an S3 bucket.

Q21)

You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process.

Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.

✓ Ensure that agent is running on the Instances.
● Check to see if the IAM user has the right permissions for EC2
✓ Check to see if the right role has been assigned to the EC2 Instances
✓ Check the Instance status by using the Health API.

Q22)

A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed.

What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service?

● Create an alias of the key
✓ Use Data key caching
● Enable rotation of the keys
● Use the right key policy

Q23)

You have an EBS volume attached to an EC2 Instance which uses KMS for Encryption.

Someone has now gone ahead and deleted the Customer Key which was used for the EBS encryption. What should be done to ensure the data can be decrypted.

● Request AWS Support to recover the key
✓ Copy the data from the EBS volume before detaching it from the Instance
● Create a new Customer Key using KMS and attach it to the existing volume
● Use AWS Config to recover the key

Q24) TPT Limited hosts multiple resources using AWS service. Robert is working as a security administrator notices an incident of a suspicious API activity which occurred 11 days ago. How should Robert get the API activity from that point in time?

● Use AWS Config to get the API calls which were made 11 days ago.
● Search the Cloud Watch metrics to find for the suspicious activity which occurred 11 days ago
● None of these
✓ Search the Cloudtrail event history on the API events which occurred 11 days ago.
● Search the Cloud Watch logs to find for the suspicious activity which occurred 11 days ago

Q25) Which of the following options ensures encrypted cloudtrail logs being delivered in the AWS account?

● Enable KMS encryption for the logs which are sent to Cloudwatch
● Enable S3-KMS for the underlying bucket which receives the log files
● None of these
● Enable S3-SSE for the underlying bucket which receives the log files
✓ Don't do anything since Cloud trail logs are automatically encrypted.

Q26) Which of the following options helps to serve up private content using the keys available with Cloudfront?

● Add the keys to the S3 bucket
✓ Create pre-signed URL's
● Use AWS Access keys
● None of these
● Add the keys to the backend distribution.

Q27)

You are building a system to distribute confidential training videos to employees.

Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly accessible from S3 directly?

● Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).
● Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
● Add the CloudFront account security group "amazon-cf/amazon-cf-sg?? to the appropriate S3 bucket policy.
✓ Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

Q28) TPT Limited has an application using DynamoDB table. A compliance requirement wants to ensure that all data should be encrypted at rest. Which of the given options will help to achieve the above requirement?

● Encrypt the table using AWS KMS after it is created
✓ Encrypt the table using AWS KMS before it is created
● None of these
● Use the AWS SDK to encrypt the data before sending it to the DynamoDB table
● Use S3 buckets to encrypt the data before sending it to DynamoDB

Q29)

Your company hosts critical data in an S3 bucket. There is a requirement to ensure that all data is encrypted.

There is also metadata about the information stored in the bucket that needs to be encrypted as well.

Which of the below measures would you take to ensure this requirement is fulfilled?

✓ Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time.
● Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server KMS encryption.
● Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server side encryption.
● Put the metadata in the S3 bucket itself.

Q30)

One of the EC2 Instances in your company has been compromised.

What steps would you take to ensure that you could apply digital forensics on the Instance. Select 2 answers from the options given below

✓ Ensure that the security groups only allow communication to this forensic instance
✓ Create a separate forensic instance
● Remove the role applied to the Ec2 Instance
● Terminate the instance

Q31)

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol.

There is a security mandate that all traffic between the client and the EC2 Instances need to be secure.

How would you accomplish this?

✓ Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances
● Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
● Use a Classic Load balancer and terminate the SSL connection at the ELB
● Use an Application Load balancer and terminate the SSL connection at the ELB

Q32) TPT Limited hired Robert as a third-party security auditor. The company wants to provide read-only access to all AWS resources and logs of all VPC records and events that have occurred on AWS. Which of the following is the best possible option to meet the auditors requirement without compromising on security in the AWS environment?

● Create a role that has the required permissions for the auditor.
● Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
● The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.
✓ Enable CloudTrail logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.
● None of these

Q33)

Your company hosts a large section of EC2 instances in AWS. There are strict security rules governing the EC2 Instances.

During a potential security breach , you need to ensure quick investigation of the underlying EC2 Instance.

Which of the following service can help you quickly provision a test environment to look into the breached instance.

● AWS Cloudtrail
● AWS Cloudformation

✓ AWS Cloudwatch
● AWS Config

Q34)

Your company has a set of EBS volumes defined in AWS. The security mandate is that all EBS volumes are encrypted.

What can be done to notify the IT admin staff if there are any unencrypted volumes in the account.

● Use AWS Lambda to check for the unencrypted EBS volumes
● Use AWS Guard duty to check for the unencrypted EBS volumes
✓ Use AWS Config to check for unencrypted EBS volumes
● Use AWS Inspector to inspect all the EBS volumes

Q35)

Your company use AWS KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities.

What can be done during the deletion process to verify that the key is no longer being used.

● Rotate the keys once before deletion to see if other services are using the keys
● Use Key policies to see the access level for the keys
✓ Use CloudTrail to see if any KMS API request has been issued against existing keys
● Change the IAM policy for the keys to see if other services are using the keys

Q36)

Your company has just started using AWS and created an AWS account. They are aware of the potential issues when root access is enabled.

How can they best safeguard the account when it comes to root access? Choose 2 answers from the options given below

● Change the password for the root account.
✓ Create an Admin IAM user with the necessary permissions
● Delete the root access account
✓ Delete the root access keys

Q37)

You have a bucket and a VPC defined in AWS. You need to ensure that the bucket can only be accessed by the VPC endpoint.

How can you accomplish this?

✓ Modify the bucket Policy for the bucket to allow access for the VPC endpoint
● Modify the IAM Policy for the bucket to allow access for the VPC endpoint
● Modify the route tables to allow access for the VPC endpoint
● Modify the security groups for the VPC to allow access to the S3 bucket