Answer Sheet

Q1)

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

---

Q2)

A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resources for their infrastructure.

They want to ensure that the EC2 Instances don't have any high security vulnerabilities.

They want to ensure a complete DevSecOps process. How can this be achieved?

- Use AWS Trusted Advisor API's in the pipeline for the EC2 Instances
- ✓ Use AWS Inspector API's in the pipeline for the EC2 Instances
- Use AWS Config to check the state of the EC2 instance for any sort of security issues.
- Use AWS Security Groups to ensure no vulnerabilities are present

---

Q3)

You want to track access requests for a particular S3 bucket.

How can you achieve this in the easiest possible way?

- Enable Cloudwatch logs for the bucket
- Enable Cloudwatch metrics for the bucket
- ✓ Enable server access logging for the bucket
- Enable AWS Config for the S3 bucket

Q4)

You have just developed a new mobile application that handles analytics workloads on large scale datasets that are stored on Amazon Redshift.

Consequently, the application needs to access Amazon Redshift tables. Which of the below methods would be the best, both practically and security-wise, to access the tables?

Choose the correct answer from the options below

- ✓ Use roles that allow a web identity federated user to assume a role that allows access to the RedShift table by providing temporary credentials.
- Create a RedShift read-only access policy in IAM and embed those credentials in the application.
- Create an HSM client certificate in Redshift and authenticate using this certificate.
- Create an IAM user and generate encryption keys for that user. Create a policy for RedShift read-only access. Embed the keys in the application.

Q5)

Your team is designing a web application. The users for this web application would need to sign in via an external ID provider such as facebook or Google.

Which of the following AWS service would you use for authentication?

- AWS IAM
- AWS SAML
- ✓ AWS Cognito
- AWS Config

Q6)

DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic.

Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a "WAF sandwich."

Which of the following statements best describes what a "WAF sandwich" is? Choose the correct answer from the options below

- ✓ The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers.

- The EC2 instance running your WAF software is placed between your public subnets and your private subnets.
- The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
- The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the Internet.

Q7)

Your company has a hybrid environment , with on-premise servers and servers hosted in the AWS cloud. They are planning to use the Systems

Manager for patching servers. Which of the following is a pre-requisite for this to work?

- Ensure that an IAM User is created
- ✅ Ensure that an IAM service role is created
- Ensure that the on-premise servers are running on Hyper-V.
- Ensure that an IAM Group is created for the on-premise servers

---

Q8)

An employee keeps terminating EC2 instances on the production environment.

You've determined the best way to ensure this doesn't happen is to add an extra layer of defence against terminating the instances.

What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below

- Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
- Modify the IAM policy on the user to require MFA before deleting EC2 instances
- ✅ Tag the instance with a production-identifying tag and modify the employees group to allow only start, stop, and reboot API calls and not the terminate instance call.
- ✅ Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.

Q9)

You have been given a new brief from your supervisor for a client who needs a web application set up on AWS. The most important requirement is that

MySQL must be used as the database, and this database must not be hosted in the public cloud, but rather at the client's data center due to security risks.

Which of the following solutions would be the best to assure that the client's requirements are met? Choose the correct answer from the options below

- Build the application server on a public subnet and build the database in a private subnet with a secure ssh connection to the private subnet from the client's data center.
- Build the application server on a public subnet and the database on a private subnet with a NAT instance between them.
- Use the public subnet for the application server and use RDS with a storage gateway to access and synchronize the data securely from the local data center.
- ✅ Build the application server on a public subnet and the database at the client's data center. Connect them with a VPN connection which uses IPsec.

Q10)

Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used.

They have hired an external vendor for analyzing their log files. They have their own AWS account.

What is the best way to ensure that the partner account can access the log files in the company account for analysis.Choose 2 answers from the options given below

- Ensure the IAM user has access for read-only to the S3 buckets
- ✅ Create an IAM Role in the company account
- Create an IAM user in the company account
- ✅ Ensure the IAM Role has access for read-only to the S3 buckets

---

Q11)

Your company has been using AWS for hosting EC2 Instances for their web and database applications.

They want to have a compliance check to see the following

• Whether any ports are left open other than admin ones like SSH and RDP

• Whether any ports to the database server other than ones from the web server security group are open

Which of the following can help achieve this in the easiest way possible. You don't want to carry out an extra configuration changes?

- AWS Inspector
- ✅ AWS Trusted Advisor
- AWS Config

- AWS GuardDuty

Q12) Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below

- ✓ AWS Application Load Balancer
- AWS Lambda
- ✓ AWS Cloudfront
- AWS Classic Load Balancer

Q13)

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC.

Your server's on-premises will be communicating with your VPC instances. You will be establishing IPSec tunnels over the internet.

You will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways.

Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above? Choose 4 answers form the options below

- ✓ Peer identity authentication between VPN gateway and customer gateway
- ✓ Protection of data in transit over the Internet
- ✓ Data encryption across the Internet
- End-to-end Identity authentication
- End-to-end protection of data in transit
- ✓ Data integrity protection across the Internet

Q14)

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16.

The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306.

The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). which of the below mentioned entries is required in the private subnet database security group DBSecGrp?

- Allow Outbound on port 3306 for Destination Web Server Security Group WebSecGrp.
- Allow Inbound on port 3306 from source 20.0.0.0/16
- ✓ Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp.
- Allow Outbound on port 80 for Destination NAT Instance IP

Q15)

Your developer is using the KMS service and an assigned key in their Java program.They get the below error when running the code

arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey

Which of the following could help resolve the issue?

- Ensure that UserB is given the right permissions in the Bucket policy
- ✓ Ensure that UserB is given the right permissions in the Key policy
- Ensure that UserB is given the right permissions in the IAM policy
- Ensure that UserB is given the right IAM role to access the key

Q16)

An organization has launched 5 instances: 2 for production and 3 for testing.

The organization wants that one particular group of IAM users should only access the test instances and not the production ones.

How can the organization set that as a part of the policy?

- ✓ Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags
- Create an IAM policy with a condition which allows access to only small instances
- Define the IAM policy which allows access based on the instance ID
- Launch the test and production instances in separate regions and allow region wise access to the group

Q17)

Your company is planning on AWS on hosting its AWS resources.

There is a company policy which mandates that all security keys are completed managed within the company itself.

Which of the following is the correct measure of following this policy?

- ✓ Generating the key pairs for the EC2 Instances using puttygen
- Using the AWS KMS service for creation of the keys and the company managing the key lifecycle thereafter.
- Use the EC2 Key pairs that come with AWS
- Use S3 server-side encryption

Q18)

You have setup a set of applications across 2 VPC's. You have also setup VPC Peering. The applications are still not able to communicate across the Peering connection.

Which network troubleshooting steps should be taken to resolve the issue?

- Check to see if the VPC has a NAT gateway attached.
- Check to see if the VPC has an Internet gateway attached.
- Ensure the applications are hosted in a public subnet
- ✓ Check the Route tables for the VPC's

Q19)

A company requires that data stored in AWS be encrypted at rest.

Which of the following approaches achieve this requirement? Select 2 answers from the options given below.

- When storing data in Amazon S3, use object versioning and MFA Delete.
- ✓ When storing data in EBS, encrypt the volume by using AWS KMS.
- When storing data in Amazon EBS, use only EBS–optimized Amazon EC2 instances.
- ✓ When storing data in S3, enable server-side encryption.

Q20)

You need to ensure that objects in an S3 bucket are available in another region.

This is because of the criticality of the data that is hosted in the S3 bucket.

How can you achieve this in the easiest way possible?

- Create an S3 snapshot in the destination region
- Write a script to copy the objects to another bucket in the destination region
- ✓ Enable cross region replication for the bucket
- Enable versioning which will copy the objects to the destination region (Incorrect)

Q21)

A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks.

Which steps can the company use to protect their application? Select 2 answers from the options given below.

- ✓ Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
- Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
- ✓ Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
- Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.

Q22)

Your company has a set of 1000 EC2 Instances defined in an AWS Account. They want to effectively automate several administrative tasks on these instances.

Which of the following would be an effective way to achieve this?

- Use the AWS Inspector
- ✓ Use the AWS Systems Manager Run Command
- Use the AWS Systems Manager Parameter Store
- Use AWS Config (Incorrect)

Q23)

You have a set of Keys defined using the AWS KMS service.

You want to stop using a couple of keys, but are not sure of which services are currently using the keys.

Which of the following would be a safe option to stop using the keys from further usage.

- Set an alias for the key
- Change the key material for the key (Incorrect)
- ✓ Disable the keys
- Delete the keys since anyway there is a 7 day waiting period before deletion

Q24)

A security engineer must ensure that all infrastructure launched in the company AWS account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AMIs and that all attached EBS volumes are encrypted.

Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2

answers from the options given below.

- Set up a CloudWatch event based on Amazon inspector findings
- ✓ Trigger a Lambda function from a scheduled CloudWatch event that terminates non-compliant infrastructure.
- Set up a CloudWatch event based on Trusted Advisor metrics
- ✓ Monitor compliance with AWS Config Rules triggered by configuration changes

---

Q25)

A company has a legacy application that outputs all logs to a local text file.

Logs from all applications running on AWS must be continually monitored for security related messages.

What can be done to allow the company to deploy the legacy application on Amazon EC2 and still meet the monitoring requirement?

- Export the local text log files to CloudTrail. Create a Lambda function that queries the CloudTrail logs for security incidents using Athena.
- Install the Amazon Inspector agent on any EC2 instance running the legacy application. Generate CloudWatch alerts based on any Amazon Inspector findings. (Incorrect)
- ✓ Send the local text log files to CloudWatch Logs and configure a CloudWatch metric filter. Trigger cloudWatch alarms based on the metrics.
- Create a Lambda function that mounts the EBS volume with the logs and scans the logs for security incidents. Trigger the function every 5 minutes with a scheduled Cloudwatch event.
