Answer Sheet

Q1)

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

Q2)

You need to create a linux EC2 instance in AWS. Which of the following steps is used to ensure secure authentication to the EC2 instance.

Choose 2 answers from the options given below.

- ✓ Use the private key to log into the instance
- ✓ Create a key pair using putty
- Ensure to create a strong password for logging into the EC2 Instance
- Ensure the password is passed securely using SSL

Q3)

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.

Q4)

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

Q5)

Your application currently use AWS Cognito for authenticating users. Your application consists of different types of users.

Some users are only allowed read access to the application and others are given contributor access.

How would you manage the access effectively?

- You need to manage this within the application itself
- ✓ Create different cognito groups, one for the readers and the other for the contributors.
- Create different cognito endpoints , one for the readers and the other for the contributors.
- This needs to be managed via Web security tokens

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)

An auditor needs access to logs that record all API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts.

What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below

- Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.
- ✅ Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and grant the auditor access to that single bucket in the primary account.
- Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary accounts. Then grant the auditor access to the S3 bucket that receives the CloudTrail log files.
- Configure the CloudTrail service in each AWS account, and have the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary IAM account that can assume a read-only role in the secondary AWS accounts.

Q8)

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

---

Q9)

You have several S3 buckets defined in your AWS account. You need to give access to external AWS accounts to these S3 buckets.

Which of the following can allow you to define the permissions for the external accounts? Choose 2 answers from the options given below

- IAM users
- ✅ Buckets ACL's
- IAM policies
- ✅ Bucket policies

Q10)

A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS.

What could be the strategy to adopt for managing the accounts.

- Use multiple IAM roles, each group for each department
- Use multiple IAM groups, each group for each department
- Use multiple VPC's in the account, each VPC for each department
- ✅ Use multiple AWS accounts, each account for each department

---

Q11)

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.

Q12)

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.

Q13)

You are planning on using the AWS KMS service for managing keys for your application.

For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below

- ✓ Password
- Large files
- Image Objects
- ✓ RSA Keys

Q14)

A company has been using the AWS KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use.

What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below

- ✓ See Cloudtrail for usage of the key
- ✓ See who is assigned permissions to the master key
- Determine the age of the master key
- Use AWS cloudwatch events for events generated for the key

Q15) Which of the following is the correct sequence of how KMS manages the keys when used along with the Redshift cluster service

- The master keys encrypts the data encryption keys. The data encryption keys encrypts the database key
- The master keys encrypts the database key. The database key encrypts the data encryption keys.
- ✓ The master keys encrypts the cluster key. The cluster key encrypts the database key. The database key encrypts the data encryption keys.
- The master keys encrypts the cluster key, database key and data encryption keys

---

Q16)

A company wants to use Cloudtrail for logging all API activity. They want to segregate the logging of data events and management events.

How can this be achieved? Choose 2 answers from the options given below

- ✓ Create another trail that logs management events to another S3 bucket
- ✓ Create one trail that logs data events to an S3 bucket
- Create one Cloudtrail log group for data events
- Create another Cloudtrail log group for management events

Q17)

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

---

Q18)

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

Q19)

A company is planning on using AWS for hosting their applications.

They want complete separation and isolation of their production, testing and development environments.

Which of the following is an ideal way to design such a setup?

- [x] Use separate AWS accounts for each of the environments
- [ ] Use separate IAM Policies for each of the environments
- [ ] Use separate IAM Roles for each of the environments
- [ ] Use separate VPC's for each of the environments

Q20)

An application is designed to run on an EC2 Instance. The applications needs to work with an S3 bucket.

From a security perspective, what is the ideal way for the EC2 instance/ application to be configured?

- [x] Assign an IAM Role and assign it to the EC2 Instance
- [ ] Assign an IAM user to the application that has specific access to only that S3 bucket
- [ ] Use the AWS access keys ensuring that they are frequently rotated.
- [ ] Assign an IAM group and assign it to the EC2 Instance

Q21)

Your company has an EC2 Instance hosted in AWS. This EC2 Instance hosts an application.

Currently this application is experiencing a number of issues. You need to inspect the network packets to see what the type of error that is occurring?

Which one of the below steps can help address this issue?

- [x] Use a network monitoring tool provided by an AWS partner.
- [ ] Use another instance. Setup a port to "promiscuous mode" and sniff the traffic to analyze the packets.
- [ ] Use the VPC Flow Logs.
- [ ] Use Cloudwatch metric

Q22)

Which of the below services can be integrated with the AWS Web application firewall service.

Choose 2 answers from the options given below

- [x] AWS Application Load Balancer
- [ ] AWS Lambda
- [x] AWS Cloudfront
- [ ] AWS Classic Load Balancer

Q23)

A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion.

What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below

- [x] Enable MFA Delete in the bucket policy
- [ ] Enable data at rest for the objects in the bucket
- [x] Enable versioning on the S3 bucket
- [ ] Enable data in transit for the objects in the bucket

Q24)

You company has mandated that all data in AWS be encrypted at rest. How can you achieve this for EBS volumes?

Choose 2 answers from the options given below

- [ ] Enable encryption on existing EBS volumes
- [x] Use TreuEncrypt for Linux based instances
- [x] Use Windows Bitlocker for windows-based instances
- [ ] Use AWS KMS to encrypt the existing EBS volumes

Q25)

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

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

Q26) In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement

- [ ] Data keys from AWS KMS
- [x] SSL from your application
- [ ] Transparent data encryption
- [ ] Data Keys from CloudHSM

Q27) Which of the following is the responsibility of the customer? Choose 2 answers from the options given below.

- [ ] Decommissioning of old storage devices
- [x] Protection of data in transit
- [x] Encryption of data at rest
- [ ] Management of the Edge locations

Q28)

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
- [x] 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

---

Q29)

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
- [x] Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp.
- [ ] Allow Outbound on port 80 for Destination NAT Instance IP

Q30)

A user has enabled versioning on an S3 bucket. The user is using server side encryption for data at Rest.

If the user is supplying his own keys for encryption SSE-C., which of the below mentioned statements is true?

- [ ] AWS S3 does not allow the user to upload his own keys for server side encryption
- [x] It is possible to have different encryption keys for different versions of the same object
- [ ] The user should use the same encryption key for all versions of the same object
- [ ] The SSE-C does not work when versioning is enabled

Q31)

You are planning to use AWS Config to check the configuration of the resources in your AWS account.

You are planning on using an existing IAM role and using it for the AWS Config resource.

Which of the following is required to ensure the AWS config service can work as required?

- [ ] Ensure that there is a user policy in place for the AWS Config service within the role
- [ ] Ensure that there is a grant policy in place for the AWS Config service within the role
- [x] Ensure that there is a trust policy in place for the AWS Config service within the role
- [ ] Ensure that there is a group policy in place for the AWS Config service within the role

---

Q32)

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

---

Q33)

Your company has an external web site. This web site needs to access the objects in an S3 bucket.

Which of the following would allow the web site to access the objects in the most secure manner?

- Use the aws:sites key in the condition clause for the bucket policy
- ✓ Use the aws:Referer key in the condition clause for the bucket policy
- Grant public access for the bucket via the bucket policy
- Grant a role that can be assumed by the web site

Q34)

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

---

Q35)

You are building a large-scale confidential documentation web server on AWS and all of the documentation for it will be stored on S3.

One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use CloudFront to accomplish this.

Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below

- Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).
- Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
- ✓ Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM User.

Q36)

Your company makes use of S3 buckets for storing data. There is a company policy that all services should have logging enabled.

How can you ensure that logging is always enabled for created S3 buckets in the AWS Account?

- Use AWS Cloudwatch metrics to check whether logging is enabled for buckets
- ✓ Use AWS Config Rules to check whether logging is enabled for buckets
- Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
- Use AWS Cloudwatch logs to check whether logging is enabled for buckets

---

Q37)

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

---

Q38)

A company has external vendors that must deliver files to the company. These vendors have cross-account that gives them permission to upload objects to one of the company's S3 buckets.

What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below

- Encrypt the object with a KMS key controlled by the company.

- [x] Add a grant to the object's ACL giving full permissions to bucket owner.
- [ ] Attach an IAM role to the bucket that grants the bucket owner full permissions to the object
- [x] Upload the file to the company's S3 bucket as an object

Q39)

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.
- [x] 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)

Q40)

A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be rotated annually.

What two methods can the security team use to rotate each key? Select 2 answers from the options given below

- [ ] Use the CLI or console to explicitly rotate an existing CMK
- [ ] Import new key material to an existing CMK
- [x] Enable automatic key rotation for a CMK
- [x] Import new key material to a new CMK; Point the key alias to the new CMK.

Q41)

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?

- [x] 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)

Q42)

Your current setup in AWS consists of the following architecture. 2 public subnets, one subnet which has the web servers accessed by users across the internet and the other subnet for the database server.

Which of the following changes to the architecture would add a better security boundary to the resources hosted in your setup

- [ ] Consider moving both the web and database server to a private subnet
- [x] Consider moving the database server to a private subnet
- [ ] Consider moving the web server to a private subnet
- [ ] Consider creating a private subnet and adding a NAT instance to that subnet

Q43)

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
- [x] Enable Cross region replication for the S3 bucket

Q44)

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. (Incorrect)
- [ ] Use the AWS Config tool to manage the permissions for the different users
- [x] 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

Q45)

A company hosts data in S3. There is a requirement to control access to the S3 buckets.

Which are the 2 ways in which this can be achieved?

- [x] Use IAM user policies
- [ ] Use the Secure Token service
- [x] Use Bucket policies
- [ ] Use AWS Access Keys

Q46)

Your IT Security team has identified a number of vulnerabilities across critical EC2 Instances in the company's AWS Account.

Which would be the easiest way to ensure these vulnerabilities are remediated?

- [ ] Use AWS Inspector to patch the servers
- [ ] Use AWS CLI commands to download the updates and patch the servers.
- [ ] Create AWS Lambda functions to download the updates and patch the servers.
- [x] Use AWS Systems Manager to patch the servers

Q47)

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?

- [x] 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

---

Q48)

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?

- [x] 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

Q49)

A company hosts a critical web application on the AWS Cloud. This is a key revenue generating application for the company.

The IT Security team is worried about potential DDos attacks against the web site.

The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack.

What should be done in this regard?

- [x] Consider using the AWS Shield Advanced Service
- [ ] Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack. (Incorrect)
- [ ] Consider using the AWS Shield Service
- [ ] Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.

Q50)

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
- [x] Check the Route tables for the VPC's

Q51)

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.
- [x] 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.
- [x] When storing data in S3, enable server-side encryption.

Q52)

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)

Q53)

You want to ensure that you keep a check on the Active EBS Volumes, Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit.

Which of the below services can help in this regard?

- ✓ AWS Trusted Advisor
- AWS EC2
- AWS Cloudwatch
- AWS SNS

Q54)

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.

Q55)

Every application in a company's portfolio has a separate AWS account for development and production.

The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services.

How can they control this functionality?

- Create an IAM policy that denies access to the services. Create a Config Rule that checks that all users have the policy assigned. Trigger a Lambda function that adds the policy when found missing.
- Create a Service Control Policy that denies access to the services. Apply the policy to the root account.
- Create an IAM policy that denies access to the services. Associate the policy with an IAM group and enlist all users and the root users in this group. (Incorrect)
- ✓ Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit.

Q56)

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.

Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below

- A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.
- ✓ A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports
- A network ACL with a rule that allows outgoing traffic on port 443.
- ✓ A security group with a rule that allows outgoing traffic on port 443

Q57)

You working in the media industry and you have created a web application where users will be able to upload photos they create to your website.

This web application must be able to call the S3 API in order to be able to function.

Where should you store your API credentials whilst maintaining the maximum level of security?

- Save your API credentials in a public Github repository.
- ✓ Don't save your API credentials. Instead create a role in IAM and assign this role to an EC2 instance when you first create it.

- Save the API credentials to your PHP files.
- Pass API credentials to the instance using instance userdata. (Incorrect)

Q58)

A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored.

Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived.

Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.

- ✓ Ensure a lifecycle policy is defined on the S3 bucket to move the data to Amazon Glacier after 6 months.
- Ensure a lifecycle policy is defined on the S3 bucket to move the data to EBS volumes after 6 months.
- ✓ Enable CloudTrail logging in all accounts into S3 buckets
- Enable CloudTrail logging in all accounts into Amazon Glacier

Q59)

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)

Q60)

You want to launch an EC2 Instance with your own key pair in AWS. How can you achieve this? Choose 2 answers from the options given below.

Each option forms part of the solution.

- ✓ Import the public key pair into EC2
- Create a new key pair using the AWS CLI
- ✓ Use a third party tool to create the Key pair
- Import the private key pair into EC2