**Answer Sheet**

**Q1)**

**You want to use CloudWatch Events to enable automated responses to specific actions taken in your AWS account.**

**Which of these could not be used as a target for CloudWatch Events?**

- ECS tasks
- ✅ S3

**Explanation:-**S3 is not compatible with CloudWatch Events as a target.

- EC2
- SNS Queues

---

**Q2) In order to enable CloudFront access logs on a distribution, which S3 bucket ACLs are required to be in place? (pick two)**

- awslogsdelivery account WRITE_ACP
- ✅ account FULL.CONTROL

**Explanation:-**To enable CloudFront access logs, the owner of the distribution must have full access to the bucket, and the process of enabling the logs will create a new bucket ACL granting full access to the awslogsdelivery account.

- ✅ awslogsdelivery account FULL_CONTROL

**Explanation:-**To enable CloudFront access logs, the owner of the distribution must have full access to the bucket, and the process of enabling the logs will create a new bucket ACL granting full access to the awslogsdelivery account.

- account WRITE.ACP

---

**Q3)**

**Your company offers a streaming service that sends application logs to CloudWatch Logs, and you want to configure monitoring for it.**

**How would you configure the Amazon Kinesis service to ingest CloudWatch Logs, and have them pushed to S3?**

- Enable Kinesis Data Firehose error logging in the Kinesis Data Firehose console, and select ElasticSearch as the delivery destination
- Enable Kinesis Data Firehose error logging in the Kinesis Data Firehose console, and select RedShift as the delivery destination
- ✅ Configure a Kinesis Data Firehose with a subscription filter to the CloudWatch log group, and select S3 as the delivery destination

**Explanation:-**Kinesis Data Firehose can subscribe to a CloudWatch log group, ingesting all log entries with the option to buffer and batch the output to a delivery destination such as S3.

- Create a Kinesis Video Stream, and select S3 as the delivery destination

---

**Q4)**

**Your company is deploying a new application into AWS and would like to choose a platform with no single points of failure. The application requires a load balancer, and a web/app tier running Nginx and Java.**

**Which of the following solutions meets the requirement with the least amount of operational overhead?**

- ✅ Deploy the code into an Elastic Beanstalk application

**Explanation:-**Elastic Beanstalk, when configured appropriately, has no single points of failure, and very few operational tasks (See module 3, lesson 6.8 Elastic Beanstalk)

- Deploy the code on EC2 instances managed by the IT operations team
- Deploy the code as Lambda functions, and implement API Gateway as the front end
- Deploy the code on-premises using Docker containers and manage via EKS

---

**Q5)**

**You are designing a new EC2 application cluster that will be used at your company. This fleet will receive a medium amount of traffic and will only serve simple functions.**

**You have been instructed to make the infrastructure as cost effective as possible.**

**Which of these practices are highly efficient and cost effective? (pick two)**

- Create an autoscaling steady-state group to maintain the same number of instances at all times
- ✅ Use T2 instances with T2 unlimited enabled to maintain performance

**Explanation:-**(See module 3, lesson 6.4 Auto Scaling)

- Attach a Provisioned IOPS SSD (iol) EBS volume tyour instance for data storage
- ✅ Configure your autoscaling policies treduce the number of instances being used during slow traffic hours

**Explanation:-**(See module 3, lesson 6.4 Auto Scaling)

---

**Q6)**

**You have a singleton application that can only run on a single instance with a static public IP, and is not a candidate for horizontal scaling.**

**You've been tasked with improving the availability of this application while retaining the current single deployment on a c5.large instance.**

**Which of the following choices improve availability while meeting the other requirements?**

- Create an AMI of the instance and configure an Auto Scaling group to operate in a steady state of 1 instance
- Configure a CloudWatch alarm to send email if the instance becomes unavailable
- ✅ Enable EC2 Auto Recovery on the instance

**Explanation:-**EC2 Auto Recovery will reboot or stop/start the instance if it fails its reachability checks, while maintaining the same instance ID and all IP information such as an EIP attachment.

- Configure third-party monitoring to send email if the instance becomes unreachable

---

**Q7)**

**You are designing a storage system to be used by Linux-based EC2 instances. The instances are in different availability zones but within the same VPC, and will need scalable, shared file storage.**

**Which is the best storage service to use for this?**

- Amazon Elastic Block Storage (EBS)
- Amazon Glacier
- Amazon S3
- ✅ Amazon Elastic File System (EFS)

**Explanation:-**EFS is a highly scalable storage service that works for Unix-based servers. EFS can be attached to EC2 instances within the same VPC even if they're in different availability zones, and can scale up to a petabyte of data. EFS scales to use only the storage you are currently using.

---

**Q8)**

**You have a web server fleet that routinely experiences peak traffic from 5 PM until 8 PM.**

**How should you configure your auto scaling to meet these conditions using automation? (Pick two)**

- ✅ Configure a scheduled action to scale out and in every day around the peak time

**Explanation:-**Both auto scaling policies and scheduled actions are reasonable automated solutions to meet the requirements.

- ✅ Configure an autoscaling policy to be triggered by high CPU usage across the fleet

**Explanation:-**Both auto scaling policies and scheduled actions are reasonable automated solutions to meet the requirements.

- Scale manually every day using the AWS console
- Configure your auto scalling group to maintain a state at all times

---

**Q9)**

**You manage dozens of EC2 instances for your company, and you notice that you are spending more time provisioning and configuring your EC2 instances than anything else during your day.**

**Which AWS services could you utilize to streamline this process? (pick two)**

- Athena
- Route 53
- ✅ OpsWorks

**Explanation:-**Both of these services utilize IAC (Infrastructure as Code) concepts to deploy and maintain infrastructure such as EC2 instances with little manual effort.

- CloudWatch
- ✅ CloudFormation

**Explanation:-**Both of these services utilize IAC (Infrastructure as Code) concepts to deploy and maintain infrastructure such as EC2 instances with little manual effort.

---

**Q10)**

**You have deployed your Auto Scaling group into multiple AZ within the same region, and due to a weather event, an entire AZ becomes unavailable.**

**What can you expect your Auto Scaling group to do to maintain capacity?**

- ✅ Launch new instances in a different AZ

**Explanation:-**The Auto Scaling service will maintain the desired number of instances even if it needs to deploy all of them into a single AZ due to an outage. (See module 4 lesson 7.2 Provisioning Resources in AWS)

- Notify you that the instances have gone out and wait for instruction
- Launch new instances in the same AZ
- Wait for you to manually launch new instances

---

**Q11)**

**You are designing a new CloudFormation template for creating VPC resources.**

**Which of the following sections of the CloudFormation template are required for the template to be usable?**

- ✅ Resources

**Explanation:-**The Resources section declares the AWS resources that you want to include in the stack, such as an Amazon EC2 instance or an Amazon S3 bucket, and it is the only required section of the template.

- Metadata
- Parameters
- Outputs

---

**Q12)**

**You have been tasked with updating a Beanstalk app on a large number of instances, and would like to deploy a new AMI containing the latest security updates.**

**Which AWS Beanstalk feature would you employ to meet the requirement?**

- Elastic Beanstalk Rolling Deployments
- ✅ Elastic Beanstalk Rolling Updates

**Explanation:-**Elastic Beanstalk has the capability to update instances in batches as long as they are within the same region, and rolling updates will launch new EC2 instances as part of the update, replacing all EC2 resources in the application.

- Elastic Beanstalk Rolling Installs
- Elastic Beanstalk Rolling Patches

---

**Q13)**

**You have been tasked with updating an Elastic Beanstalk application, but you need to retain the underlying EC2 instances.**

**Which AWS Beanstalk feature would you employ to meet the requirement?**

- Elastic Beanstalk Rolling Installs
- ✅ Elastic Beanstalk Rolling Deployments

**Explanation:-**Elastic Beanstalk has the capability to update instances in batches as long as they are within the same region, and rolling deployments maintain the same instances.

- Elastic Beanstalk Rolling Updates
- Elastic Beanstalk Rolling Patches

---

**Q14)**

**Your company has a cluster of instances, all based in the same region that are performing identical functions.**

**You would like to utilize Auto Scaling for the instances, but you must avoid any interruption of service during the implementation.**

**Which of the following methods meets this requirement?**

- Create the new Auto Scaling Group in a different region to avoid any conflict, then reconfigure clients to use the newly launched instances
- ✅ Create the new Auto Scaling Group with desired configuration, then attach the existing instances to it

**Explanation:-**Auto Scaling groups support the addition of existing instances. This is the way to ensure a seamless transition, and from there, further migration tasks can be performed with no interruption of service.

- Create the new Auto Scaling Group, then configure clients to use the newly launched instances
- None of these

---

**Q15)**

**One of your EC2 instances is showing the status as Impaired", but the rest of the instances in the AZ are healthy.**

**What can you expect Auto Scaling service to do?**

- Launch a new instance to replace the impaired instance in the same AZ, and terminate the old one
- Launch a new instance to replace the impaired instance in the same AZ, and keep the old one
- ✅ Launch a new instance to replace the impaired instance in a different AZ, and terminate the old one

**Explanation:-**The Auto Scaling service will maintain healthy instances, and when an instance fails its configured health check, it is replaced with a newly launched instance. (See mcdule 4 lesson 7.2 Provisioning Resources in AWS)

- Notify you of the impaired server and wait for further instruction

---

**Q16)**

**A company requires the latest version of the AWS CLI to be installed and validated across their EC2 inventory as well as their on-premises servers, running many different OS, including Linux and Windows.**

**What would be the most cost-effective and efficient way to deploy these packages across the hybrid fleet?**

- Use third-party tools for all nodes
- ✅ Use SSM Run Command for all nodes

**Explanation:-**SSM Run Command can be utilized for all nodes, and the execution will be quick and inexpensive (See module 4 lesson 8.1 Systems Manager Run Command)

- Use Opsworks for AWS resources, and third-party tools on-premises
- SSH loop for Linux, PowerShell remote for Windows

---

**Q17)**

**Your engineering team would like to design a fully managed, serverless infrastructure for deploying node.js applications.**

**The company does not have IT resources to dedicate to managing this environment, so the engineering team wants a solution that minimizes overhead and eliminates traditional IT infrastructure entirely.**

**Which of the following solutions accomplishes this?**

- Deploy the application using ECS on EC2
- ✅ Deploy the application using Lambda functions and CodeDeploy for updates

**Explanation:-**Only the solution using Lambda is deployed entirely serverless with no traditional IT infrastructure. All the other choices involve virtual machines with operating systems that must be managed.

- Deploy the application using Elastic Beanstalk
- Deploy the application using EKS and on-premises resources

---

**Q18)**

**Management has given your team new DR requirements that require all data stored in a second region for business continuity reasons.**

**Which of the following services are able to automatically back up your data to a remote region with no operational effort required on the part of your team? (pick two)**

- EBS Snapshots
- ✅ S3

**Explanation:-**Redshift and S3 are the only choices that allow for data to be replicated or backed up in a remote region with no chance of deletion.

- RDS
- DynamoDB
- ✅ Redshift

**Explanation:-**Redshift and S3 are the only choices that allow for data to be replicated or backed up in a remote region with no chance of deletion.

---

**Q19)**

**You have created an EBS snapshot of one of the volumes from an EC2 instance that you manage and you are trying to publicly share the snapshot, but find that you are unable to share it.**

**Which of the following could result in an EBS snapshot not being sharable?**

- The snapshot was made from an unencrypted volume
- ✅ The snapshot was created from an encrypted volume

**Explanation:-**You can share an encrypted snapshot only with specific AWS accounts. For others to use your shared, encrypted snapshot, you must also share the CMK key that was used to encrypt it. Users with access to your encrypted snapshot must create their own personal copy of it and then use that copy to restore the volume.

- The snapshot was created too soon after another snapshot was created
- You have 5 pending snapshots waiting to be created

---

**Q20)**

**We have a customer that has a web application that uses cookie-based sessions to see if users are logged in. This uses AWS Elastic Load Balancing and Auto Scaling.**

**When our load on the application increases, then Auto Scaling launches new instances for us, so load on the other instances does not decrease; therefore, all our existing users still experience slow response time.**

**What could be the cause of this? Choose the correct answer:**

- Our web app is using dynamic content features in Amazon CloudFront which is keeping our connections alive on the ELB.
- The new instances are not being added to the ELB in the process of the Auto Scale cooldown period.
- ✅ Our ELB is continuing to send the request to the web app with the previously established connections in the same backend instances rather than spreading them to the new auto scaled instances.
- Our TTL is set too high on our ELB DNS.

---

**Q21)**

**You are attempting to modify an EBS volume attached to one of your EC2 instances by decreasing the volume size but are experiencing errors.**

**What could be the problem?**

- Your EC2 instance requires a minimum EBS volume size larger than what you are trying to resize the volume to
- ✅ AWS does not allow you to decrease EBS volume size

**Explanation:-**AWS does not support decreasing EBS volume sizes. To use a smaller EBS volume, create a smaller volume and copy the data manually to the new volume.

- You are trying to decrease the size of the volume to smaller than the volume's contents
- You are logged into an account that does not have sufficient permissions

---

**Q22)**

**Your company has asked you to archive some old tax documents. These being important documents with sensitive information, you choose to use Amazon Glacier to store them because they'll be secure, but you don't need immediate access to them.**

**How long do you have to validate your lock vault policy before it expires?**

- ✅ 24 hours

**Explanation:-**You initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. Once in the inprogress state, you have 24 hours to validate your vault lock policy before the lock ID expires.

- 12 hours
- 1 hour
- 48 hours

---

**Q23)**

**You work for a company that deals with sensitive customer data that you both store and pass back and forth between EC2 instances and S3. This data must be encrypted using keys that are fully managed by the customer.**

**Which encryption methods would be ideal to maintain best security practices? (pick two)**

- SSE-AWS
- ✅ SSE-C

**Explanation:-**The correct answer choices both allow for the data encryption keys to be fully managed by the customer. SSE-KMS still uses AWS as the root CA, and SSE-AWS uses AWS for root CA, master keys, and DEK.

- SSE-KMS
- ✅ Custom client side encryption local to EC2 using keys managed by customer

**Explanation:-**The correct answer choices both allow for the data encryption keys to be fully managed by the customer. SSE-KMS still uses AWS as the root CA, and SSE-AWS uses AWS for root CA, master keys, and DEK.

---

**Q24)**

**Your application data is stored in S3, and has requirements for server-side encryption, storage in multiple regions, and master encryption keys that are controlled by your organization.**

**Which of the following actions can meet these requirements in S3? (pick four)**

- ✅ Configure bucket policies on both source and destination buckets to enforce puts and overwrites of objects with SSE-KMS enabled

**Explanation:-**Configuring default S3 encryption isn't active enforcement of the requirements, and client-side encryption does not explicitly meet the server-side encryption requirement.

- ✅ Configure cross-region replication from source to destination bucket, including choosing SSE-KMS in the destination bucket

**Explanation:-**Configuring default S3 encryption isn't active enforcement of the requirements, and client-side encryption does not explicitly meet the server-side encryption requirement.

- Configure S3 bucket default encryption as SSE-KMS
- ✅ Enable bucket versioning on both source and destination buckets

**Explanation:-**Configuring default S3 encryption isn't active enforcement of the requirements, and client-side encryption does not explicitly meet the server-side encryption requirement.

- ✅ Ensure that all source bucket objects are encrypted using SSE-KMS

**Explanation:-**Configuring default S3 encryption isn't active enforcement of the requirements, and client-side encryption does not explicitly meet the server-side encryption requirement.

- Enable client-side encryption from the application tier and encrypt the data before putting into S3

---

**Q25)**

**An application you own currently stores its data on a large EC2 root volume. You've been given a new requirement to ensure data encryption at rest.**

**What method will ensure this with the least impact on performance?**

- Create a new encrypted EFS volume and migrate the data there
- ✅ Create a new encrypted EBS volume of the same size and type as the root volume, and migrate the data to the new volume

**Explanation:-**Root volumes in EC2 cannot be encrypted natively, and so the most appropriate option is to create a new encrypted data volume that matches the size and type of the root volume to ensure similar performance.

- Leave the data on the root volume and create an encrypted volume on top of the OS for the data.
- Migrate the data to S3 with SSE-KMS

---

**Q26)**

**Your Data Science team has been given a new requirement for their data stored in Redshift: All data must be encrypted in all data warehouses.**

**Which of the following procedures can be used to bring your Redshift databases into compliance? (pick two)**

- ✅ Unload data from the database into S3, create a new encrypied database, and load the data from S3

**Explanation:-**Each of the correct answers is an appropriate way to enable encryption on a Redshift database. Both solutions take time proportional to the amount of data.

- ✅ Enable encryption in the modify cluster dialog and wait for the data to be migrated to a new, encrypted cluster

**Explanation:-**Each of the correct answers is an appropriate way to enable encryption on a Redshift database. Both solutions take time proportional to the amount of data.

- Enable encryption on the database and continue using it as usual
- Unload data from the database into S3, and query the data directly from Redshift

---

**Q27)**

**You've deployed an update to an existing customer-managed Policy, and your operations team reports that an application using that policy is no longer able to access S3.**

**What is the quickest way to restore the application to service?**

- Add static credentials with administrative access for the application to use
- Create a new Policy to approximate the previous permissions and attach to the Role used by the application
- ✅ Revert the Policy to the previous version from before your edit

**Explanation:-** customer managed policies retain 5 versions for easy rollback in case a problem is encountered.

- Restart the application to ensure it wasn't a transient problem

---

**Q28) Which of the following policy strategies would result in the best implementation of least-privilege access for remote users**

**who only connect from their home IP? (pick two)**

- One statement with a condition allowing access to 0.0.0.0/0
- ✅ One statement with a condition denying access to NotIPAddress for the remote user's home IP

**Explanation:-**IAM policies are evaluated by both explicit-allow and explicit-deny statements, and having both will ensure least-privilege even if the user is given administrative privileges through some other association.

- ✅ One statement with a condition allowing access to the remote user's home IP

**Explanation:-**IAM policies are evaluated by both explicit-allow and explicit-deny statements, and having both will ensure least-privilege even if the user is given administrative privileges through some other association.

- One statement with a condition allowing access to the public IP range of the user's ISP

---

**Q29)**

**An AWS Architect has been asked to evaluate the existing application infrastructure and propose changes that will decrease the security overhead of the application as well as increasing the resilience of overall architecture.**

**What strategies can the Architect propose before moving forward into specific change recommendations? (pick two)**

- Migrate databases to EC2 instances where they can be fully managed by the customer
- ✅ Migrate databases to AWS-managed services

**Explanation:-**The shared responsibility model for security defines that container or abstract services delegate most of the security operational overhead to AWS.

- Migrate application code to EC2 instances where they can be fully managed by the customer
- ✅ Migrate application code to AWS-managed services

**Explanation:-**The shared responsibility model for security defines that container or abstract services delegate most of the security operational overhead to AWS.

---

**Q30)**

**A security audit has been requested of your AWS account Users and the permissions granted to them.**

**Which of the following are appropriate steps to both identify overly broad access and restrict access to implement least-privilege going forward, with the least impact to existing entities? (pick two)**

- Disable API keys for all users and wait for them to complain
- Set up SAMLfederation with no-premises identity services and delegate the responsibility to the corporate IT Team
- ✅ Reduce the scope of IAM policies associated to each user by removing access to services which are not used

**Explanation:-**Least privilege access for involves a constant evolution and restriction of policies. The Access Advisor reports are a good way to assess privileges.

- ✅ Review the Access Advisor report for each User and document services to which the user has been granted privileges

**Explanation:-**Least privilege access for involves a constant evolution and restriction of policies. The Access Advisor reports are a good way to assess privileges.

---

**Q31)**

**Your company has requested that you set up an S3 bucket for each of its development teams. The access to each bucket should be restricted to just the members of each team.**

**What is the best way to configure the bucket access policies to ensure ease of access and maintenance of accesses?**

- Grant access to specific IP addresses using an S3 bucket policy
- ✅ Grant access to groups using individual customer-managed policies for each bucket

**Explanation:-**While bucket policies can also be used to achieve this goal, the management of bucket policies must be done individually, while management of resources can be performed from a central location.

- Grant user access on an individual basis using inline policy attachments
- Grant access to a specific HTTP refer using an S3 bucket policy

---

**Q32)**

**Your application uses KMS to client-side encrypt and decrypt customer data that is stored on an EFS volume. The application needs to delegate shortterm permissions to clients to decrypt individual objects on the customer side.**

**What is the most secure way to provide this access?**

- Application uses a key policy for access, clients use a separate key policy
- Application uses User static credentials for access, clients use an role
- ✅ Application uses a key policy for access, and generates grants for the clients

**Explanation:-**By using a key policy, the application gains the ability to create short-term grants for individual client applications to decrypt specific objects using the unique data encryption key for that object.

- Application uses grants for access, clients use a key policy

---

**Q33)**

**You have a requirement for end-to-end encryption of your data in transit from the end-user all the way to the application server running on EC2 in your VPC.**

**How can you accomplish this? (Pick three)**

- ✅ CloudFront with SSL enabled, Origin Protocol Policy set to SSL

**Explanation:-**If end-to-end encryption is required, it can be accomplished using several different offerings in AWS, including CloudFront and the

Application Load Balancer.
- SSL isn't required between ALB and EC2 because the network is private already
- ✅ HTTPS for the target group protocol and SSL cert installed on the EC2 application server

**Explanation:-**If end-to-end encryption is required, it can be accomplished using several different offerings in AWS, including CloudFront and the Application Load Balancer.
- ✅ ALB with SSL listener

**Explanation:-**If end-to-end encryption is required, it can be accomplished using several different offerings in AWS, including CloudFront and the Application Load Balancer.
- SSL isn't required between CloudFront and the ALB because the data only traverses the AWS network.

---

**Q34)**

**Your team has enabled GuardDuty on relevant regions in your AWS account, and are currently viewing the findings in the GuardDuty dashboard.**

**The company is expanding its use of AWS and will be creating several new accounts.**

**What is the most efficient way to track the GuardDuty findings in a multi-account scenario?**

- Bookmark the AWS Console dashboards for GuardDuty and have them all open, watching findings as they appear
- Configure CloudWatch Events in each account to forward all GuardDuty findings to a Lambda function which inserts the finding into database reachable from all accounts
- Configure CloudWatch Events in each account to forward all GuardDuty findings to an SNS topic with an email distribution list subscribed
- ✅ Designate one of the new accounts as a GuardDuty master account and invite the other accounts to become member accounts, allowing their findings to be forward to the master account automatically

**Explanation:-**GuardDuty has a great dashboard for viewing findings, and using the master/member account feature will consolidate all findings into the same dashboard with no operational overhead.

---

**Q35)**

**Your security team wants to use AWS Inspector across your EC2 instances, and wants to minimize manual effort to install the agent and run the assessments.**

**How can this be accomplished efficiently using AWS managed services and features? (pick two)**

- Use the CLI to initiate assessment runs
- ✅ Schedule the regular assessment runs straight from the Inspector dashboard on the AWS Console

**Explanation:-**AWS Inspector integrates with services like SSM Run Command for tasks like installing the agent, and jobs can be scheduled to run automatically with a few clicks in the AWS console.
- ✅ Use SSM Run Command to install the inspector agent

**Explanation:-**AWS Inspector integrates with services like SSM Run Command for tasks like installing the agent, and jobs can be scheduled to run automatically with a few clicks in the AWS console.
- Use existing third-party configure ration management tools to install the Inspector Agent

---

**Q36)**

**As part of a company migration to AWS, you've been asked to implement an audit trail :hat can be a single source of truth for auditing events in the AWS ecosystem.**

**Other requirements include ensure ng that the audit trail cannot be modified or deleted, even if the root account is compromised.**

**Which steps need to be taken to meet these requirements, assuming that AWS CloudTrail has already been identified as the best candidate? (pick four)**

- Configure CloudTrail to write to an S3 bucket in the same account
- ✅ Configure a bucket policy on the S3 bucket that denies 'deletes' and 'overwrites'

**Explanation:-**There are several good practices beyond just enabling CloudTrail on your account, and each of them can make your overall implementation more secure and ensure compliance.
- ✅ Configure CloudTrail to write to an S3 bucket in a separate account

**Explanation:-**There are several good practices beyond just enabling CloudTrail on your account, and each of them can make your overall implementation more secure and ensure compliance.
- ✅ Enable CloudTrail Log File Integrity Validation

**Explanation:-**There are several good practices beyond just enabling CloudTrail on your account, and each of them can make your overall implementation more secure and ensure compliance.
- ✅ Enable CloudTrail in all regions on the AWS account

**Explanation:-**There are several good practices beyond just enabling CloudTrail on your account, and each of them can make your overall implementation more secure and ensure compliance.
- Configure a bucket policy on the S3 bucket that requires MFA for deletes and overwrites

---

**Q37)**

**Your security team has received a new requirement to ensure compliance to policies protecting sensitive data stored in S3.**

**What recommendations can you give to meet this requirement with the least operational overhead?**

- Write a PowerShell script to parse the configuration of all S3 buckets and generate reports against buckets that have public access
- Check the S3 dashboard daily, and look for any buckets that have been flagged as public
- ✅ Enable Amazon Macie and configure on buckets containing sensitive data

**Explanation:-**Amazon Macie is designed to profile sensitive data in S3, then audit usage patterns to identify abnormal usage and generate findings.
- Enable AWS CloudTrail on the account

**Q38)**

**Your company has signed a partnership that requires IPv6 connectivity between the partner and EC2 instances inside your VPC. After adding an IPv6 range to your existing VPC, you configure IPv6 addresses on your EC2 instances.**

**The partner notifies you that they can reach your instances but aren't getting any return traffic.**

**What could be the root cause?**

- Explanation: For full bidirectional IPv6 connectivity, you can create both ingress and egress Internet gateways.
- Your VPC NAT Gateways are misconfigured
- Your VPC subnet is full
- Your VPC is missing an Internet Gateway
- ✅ Your VPC is missing an Internet egress gateway

**Explanation:-**For full bidirectional IPv6 connectivity, you can create both ingress and egress Internet gateways. (See module 7 lesson 13.2 VPC)

---

**Q39)**

**Your Wordpress web server on EC2 is experiencing periodic DDoS attacks that take the site down, requiring a reboot.**

**How can you identify the offending IPs and block the traffic in an automated fashion? (pick two)**

- Enable VPC Flow logs on the instance ENI, then manually inspect the traffic to identify DDoS sources and create NACL deny rules to match
- ✅ Put Wordpress behind a CloudFront distribution and create WAF ACLs to identify DDoS traffic and reject it.

**Explanation:-**Manual inspection will not lead to an automated solution. Using built-in features like Lambda functions and WAF ACLs will assist with a fully automated DDoS mitigation.

- Log into the EC2 instance via ssh and manually inspect the Apache logs, then create NACL deny rules to match
- ✅ Enable VPC Flow logs on the instance ENI, subscribe a Lambda function to the CloudWatch log group, use the function code to create NACL deny rules for DDoS sources

**Explanation:-**Manual inspection will not lead to an automated solution. Using built-in features like Lambda functions and WAF ACLs will assist with a fully automated DDoS mitigation.

---

**Q40)**

**You've created a VPC with cidr range 192.168.0.0/28 for a small application deployment. The VPC is deployed into a single public subnet.**

**After deploying a load balancer, and RDS instance, and an Auto Scaling group of EC2 instances, your Auto Scaling group isn't able to launch new instances.**

**What could be the root cause?**

- Your Auto Scaling group requires more than one subnet
- Your EC2 instances are launched into the wrong Security Group
- ✅ Your subnet: has used up all available IP addresses and is unable to create any more ENIs in the VPC

**Explanation:-**The VPC service supports cidr ranges from /16 to /28, and using the smallest range should be done with care, as it is relatively easy to utilize the entire range.

- Your subnet: route table is misconfigured

---

**Q41)**

**Your company has asked you to implement a scalable DLP (Data Loss Prevention) in a VPC.**

**You must inspect all outbound web traffic to make sure sensitive data isn't being sent to unauthorized destinations.**

**Which of the following solutions meet all of the requirements?**

- Apply NACL allow rules to public subjects containing NAT Gateways, only allowing traffic to appropriate destination networks
- ✅ Implement an auto-scaled group of EC2 proxy servers behind an ALB, and configure all VPC instances to use the load balancer as a proxy for outbound web traffic. Inspect requests inline and deny the requests that are not in compliance

**Explanation:-**It is the only solution that meets all of the requirements including scalability (Auto Scaling group) and inspection of all traffic (through the proxy servers)

- Launch an EC2 NAT and create outbound security group rules to authorized sites
- Launch an EC2 NAT and inspect all traffic being sent through it

---

**Q42)**

**After receiving a helpdesk request, your ops team is attempting to create a new VPC and receiving an error with a failure to create.**

**What could be the cause? (pick two)**

- You need to request new VPCs directly from AWS Support
- ✅ Your IAM user does not have the permission to create a VPCs

**Explanation:-**All AWS accounts start with a regional limit of 5 VPCs, but even if you haven't reached that, your entity still needs the appropriate permissions to create a new VPC.

- ✅ Your account is at the regional limit of 5 VPCs

**Explanation:-**All AWS accounts start with a regional limit of 5 VPCs, but even if you haven't reached that, your entity still needs the appropriate permissions to create a new VPC.

- You need to create VPCs using root credentials

---

**Q43)**

**You've been tasked with creating a multi-region network with each region's resources requiring access to each other and to AWS services.**

**How can you optimize the VPC configuration for data privacy? (Pick two)**

- Use Public IPs for cross-VPC traffic
- ✅ VPC Peering connections between the VPCs

**Explanation:-**Using VPC Endpoints will keep the traffic private, avoiding the AWS public network. VPC Peering connections are also private, even when the traffic crosses region boundaries.

- Use an IGW for AWS specific service access
- ✅ VPC Endpoints for the AWS specific service access

**Explanation:-**Using VPC Endpoints will keep the traffic private, avoiding the AWS public network. VPC Peering connections are also private, even when the traffic crosses region boundaries.

---

**Q44)**

**You have three web servers that serve similar functions, all answering to the same DNS FQDN.**

**One of them has failed its Route 53 health check, but the other two servers are still healthy.**

**You have configured your DNS failover policy to prepare for this situation using architecture best practices.**

**How will Route 53 handle this situation?**

- ✅ Stop returning the unhealthy host in the results of a DNS lookup until it passes health checks again

**Explanation:-**If you have multiple resources that perform the same function, you can configure DNS failover so that Route 53 will not return the unhealthy resources in the results of a DNS lookup, thus avoiding sending traffic to that resource.

- Terminate the existing connections of all incoming traffic to the unhealthy server
- Terminate the unhealthy server and restrict access to the two healthy servers
- Continue sending traffic to the unhealthy server until the problem is solved

---

**Q45)**

**You've deployed an Internet-facing Application Load Balancer in your VPC. After launching EC2 instances and adding them to a Target Group, you associate the Target Group with the ALB.**

**When testing the Application Load Balancer DNS endpoint from a browser, you are not getting any response.**

**What could be the cause? (pick three)**

- ✅ The Target Group health check is using the wrong port

**Explanation:-**There can be several root causes when a multi-tier application fails to function. Looking at all tiers s a good troubleshooting choice. ALBs must have correct security group rules, and the Target Group must have a correctly configured health check.

- ✅ The ALB was launched into private subnets

**Explanation:-**There can be several root causes when a multi-tier application fails to function. Looking at all tiers s a good troubleshooting choice. ALBs must have correct security group rules, and the Target Group must have a correctly configured health check.

- ✅ The EC2 instance security group does not allow inbound traffic from the ALB security group

**Explanation:-**There can be several root causes when a multi-tier application fails to function. Looking at all tiers s a good troubleshooting choice. ALBs must have correct security group rules, and the Target Group must have a correctly configured health check.

- Your VPC is missing an Ingress Internet Gateway

---

**Q46)**

**You have two EC2 instances that are in the same availability zone and the same VPC, but they can't communicate with each other.**

**What could be the root cause? (pick three)**

- ✅ The instances are attempting to use public IP addresses for communication

**Explanation:-**In order for instances inside a VPC to communicate with each other, they must have permissive security group rules, NACL rules, host-based firewall configuration and use any of the public DNS, private DNS or private IP for communication.

- ✅ One or both the servers have host-based firewall software configured to block the traffic

**Explanation:-**In order for instances inside a VPC to communicate with each other, they must have permissive security group rules, NACL rules, host-based firewall configuration and use any of the public DNS, private DNS or private IP for communication.

- You are logged in as the root account
- ✅ One or both the servers have misconfigured Security Group rules

**Explanation:-**In order for instances inside a VPC to communicate with each other, they must have permissive security group rules, NACL rules, host-based firewall configuration and use any of the public DNS, private DNS or private IP for communication.

- You are using a UNIX based server and are trying to connect to a Windows server

---

**Q47)**

**One of your most used EC2 instances routinely has trouble keeping up with traffic during peak hours. The server is an m3.large EC2 instance with a General Purpose SSD (gp2) EBS volume attached.**

**Which of these would be the easiest and most cost-effective solution?**

- Replace the EBS volume with a Throughput Optimized HDD (st1)
- Resize the instance to be an 12 server
- ✅ Upsize the instance in the M3 family until it is appropriately sized to handle the traffic

**Explanation:-**Vertical scaling of the instance is a relatively simple workflow, and does not create new resources which must then be managed. In many cases, enabling Auto Scaling could be appropriate, but not simple.

- Set stricter security policies to reduce the amount of traffic allowed to come through to the server

---

**Q48)**

**Your company is using a third-party monitoring product, and would like to make sure that all newly launched instances in an Auto Scaling group are registered with the monitoring software.**

**Which of the following solutions will ensure a fully automated solution with near real-time additions to monitoring?**

- Compose a Lambda function that is executed hourly to check for newly launched instances
- ✅ Configure an Auto Scaling lifecycle hook to trigger a Lambda function which registers the new instance

**Explanation:-**The lifecycle hook will ensure execution upon every scale-out activity, and the triggered Lambda function will add the new instance to the monitoring software in near-real time after launch.

- Check the AWS console periodically to see if any new instances were launched
- Run an AWS Inspector job to locate new instances

---

**Q49)**

**Your manager has asked for the output of "cat /etc/issue" executed on all Ubuntu EC2 instances in AWS.**

**How can you execute these commands in parallel with consolidated error logging?**

- Issue ssh commands from a single EC2 instance that loops through the inventory and executes the command on each instance
- Use userdata scripts to push the output of the command to an SNS Topic
- ✅ Utilize SSM Run Command to execute the command in parallel on EC2 instances, using predefined EC2 tags for OS type

**Explanation:-**SSM Run Command provides a centralized location to view error on command output, with the ability to execute commands in parallel or in phases.

- Use Data Pipeline to launch and EMR cluster to execute the commands in parallel

---

**Q50)**

**Your operations team would like to execute a daily job to identify orphaned EBS snapshots from deregistered AMIs in certain regions and delete them.**

**How can you accomplish this in a way that is cost-effective and low operational overhead?**

- Compose a shell script using the CLI and execute the script daily via cron on an EC2 instance
- Use the AWS Console to identify the orphaned snapshots and delete them
- ✅ Compose a Lambda function to perform the work, attach an appropriate Role to the function, and use a time-based trigger to execute it daily

**Explanation:-**Using a managed service to execute the job with quality assurance is both cost-effective and low operational overhead.

- Compose a PowerShell script and run the script daily on a local Windows server

---