Answer Sheet

Q1) What is required to enable application and operating system generated logs and publish to CloudWatch Logs?

- Syslog
- enable access logs
- IAM cross-account enabled
- ✅ CloudWatch Log Agent

Explanation:-To collect logs from your Amazon EC2 instances and on-premises servers into CloudWatch Logs, AWS offers two options: Recommended – The unified CloudWatch agent. It enables you to collect both logs and advanced metrics with one agent. It offers support across operating systems, including servers running Windows Server. Refer: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_GettingStarted.html

---

Q2) What is the purpose of VPC Flow Logs?

- Monitor netflow data from subnets
- Monitor network performance
- ✅ Capture IP traffic on network interfaces

Explanation:-VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination. Refer: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#:~:text=VPC%20Flow%20Logs%20is%20a,data%20in%20the%20chosen%20destination.

- Capture VPC error messages
- Enable Syslog services for VPC

Q3) What feature enables CloudWatch to manage capacity dynamically for EC2 instances?

- Elastic Load Balancer
- ✅ Auto-Scaling

Explanation:-Amazon EC2 Auto Scaling is a fully managed service designed to launch or terminate Amazon EC2 instances automatically to help ensure you have the correct number of Amazon EC2 instances available to handle the load for your application. Amazon EC2 Auto Scaling helps you maintain application availability through fleet management for EC2 instances, which detects and replaces unhealthy instances, and by scaling your Amazon EC2 capacity up or down automatically according to conditions you define. You can use Amazon EC2 Auto Scaling to automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs. Refer: https://aws.amazon.com/ec2/autoscaling/faqs/

- Replication lag
- Vertical scaling

Q4) You've been brought in as solutions architect to assist an enterprise customer with their migration of an e-commerce platform to Amazon Virtual Private Cloud (VPC) The previous architect has already deployed a 3-tier VPC. The configuration is as follows:
VPC vpc-2f8t>C447
IGVV ig-2d8bc445
NACL acl-2080c448
Subnets and Route Tables:
Web server's subnet-258Dc44d
Application server's suDnet-248bc44c
Database server's subnet-9189c6f9
Route Tables: rrb-218DC449rtb-238bc44b
Associations:
subnet-258bc44d: rtb-2i8bc449
Subnet-248DC44C rtb-238tX44b
subnet-9189c6f9 rtb-238Dc 44b
You are now ready to begin deploying EC2 instances into the VPC Web servers must have direct access to the internet Application and database servers cannot have direct access to the internet.
Which configuration below will allow you the ability to remotely administer your application and database servers, as well as allow these servers to retrieve updates from the Internet?

- Create a bastion and mat instance in suDnet-258Dc44d and add a route from rtD238Dc44D to the mat instance.
- Add a route from rtD-238bc44D to igw-2d8bc445 and add a bastion and NAT instance within suonet-248bc44c
- Create a bastion and MAT Instance In subnet-258bc44d. Add a route from rtb-238bc44b to igw-2d8bc445. And a new NACL that allows access between subnet-258bc44d and subnet-248bc44c.
- ✅ Create a bastion and NAT Instance in subnet-248bc44c and add a route from rtb238bc44b to subnet-258bc44d

---

Q5)

You are designing an intrusion detection prevention (IDS/IPS) solution for a customer web application in a single VPC. You are considering the options for implementing IOS IPS protection for traffic coming from the Internet.

Which of the following options would you consider? (Choose 2 answers)

- ✅ Implement a reverse proxy layer in front of web servers and configure IDS/IPS agents on each reverse proxy server.
- ✅ Implement Elastic Load Balancing with SSL listeners In front of the web applications
- Implement IDS/IPS agents on each Instance running In VPC
- Configure an instance in each subnet to switch its network interface card to promiscuous mode and analyze network traffic.

Q6) Your company previously configured a heavily used, dynamically routed VPN connection between your on-premises data center and AWS. You recently provisioned a DirectConnect connection and would like to start using the new connection. After configuring DirectConnect settings in the AWS Console, which of the following options win provide the most seamless transition for your users?

- ✅ Configure your DireclConnect router, update your VPC route tables to point to the DirectConnect connection, configure your VPN connection with a higher BGP pointy. And verify network traffic is leveraging the DirectConnect connection.
- Update your VPC route tables to point to the DirectConnect connection configure your DirectConnect router with the appropriate settings verify network traffic is leveraging DirectConnect and then delete the VPN connection.
- Configure your DireclConnect router with a higher 8GP priority man your VPN router, verify network traffic is leveraging Directconnect and then delete your existing VPN connection.

Delete your existing VPN connection to avoid routing loops configure your DirectConnect router with the appropriate settings and verity network traffic is leveraging DirectConnect.

Q7)

You are migrating a legacy client-server application to AWS The application responds to a specific DNS domain (e g www example com) and has a 2-tier architecture, with multiple application servers and a database server Remote clients use TCP to connect to the application servers. The application servers need to know the IP address of the clients in order to function properly and are currently taking that information from the TCP socket A Multi-AZ RDS MySQL instance will be used for the database. During the migration you can change the application code but you have to file a change request.

How would you implement the architecture on AWS In order to maximize scalability and high ability?

✅ File a change request to implement Alias Resource support in the application Use Route 53 Alias Resource Record to distribute load on two application servers in different AZs.
File a change request to implement Latency Based Routing support in the application Use Route 53 with Latency Based Routing enabled to distribute load on two application servers in different AZs.
File a change request to Implement Cross-Zone support in the application Use an EL8 with a TCP Listener and Cross-Zone Load Balancing enabled, two application servers in different AZs.
File a change request to implement Proxy Protocol support In the application Use an EL8 with a TCP Listener and Proxy Protocol enabled to distribute load on two application servers in different AZs.

Q8) Your company has HQ in Tokyo and branch offices all over the world and is using a logistics software with a multi-regional deployment on AWS in Japan, Europe and USA. The logistic software has a 3-tier architecture and currently uses MySQL 5.6 for data persistence. Each region has deployed its own database In the HQ region you run an hourly batch process reading data from every region to compute cross-regional reports that are sent by email to all offices this batch process must be completed as fast as possible to quickly optimize logistics how do you build the database architecture in order to meet the requirements'?

Use Direct Connect to connect all regional MySQL deployments to the HQ region and reduce network latency for the batch process
For each regional deployment, use MySQL on EC2 with a master in the region and use S3 to copy data files hourly to the HQ region
For each regional deployment, use RDS MySQL with a master in the region and send hourly RDS snapshots to the HQ region
For each regional deployment, use MySQL on EC2 with a master in the region and send hourly EBS snapshots to the HQ region
✅ For each regional deployment, use RDS MySQL with a master in the region and a read replica in the HQ region

Q9)

You have deployed a three-tier web application in a VPC with a CIOR block of 10 0 0 0/28 You initially deploy two web servers, two application servers, two database servers and one NAT instance tor a total of seven EC2 instances The web. Application and database servers are deployed across two availability zones (AZs). You also deploy an ELB in front of the two web servers, and use Route53 for DNS Web (raffle gradually increases in the first few days following the deployment, so you attempt to double the number of instances in each tier of the application to handle the new load unfortunately some of these new instances fail to launch.

Which of the following could De the root caused? (Choose 2 answers)

✅ AWS reserves the first tour and the last IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances.
✅ The ELB has scaled-up. Adding more instances to handle the traffic reducing the number of available private IP addresses for new instance launches.
AWS reserves the first and the last private IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances.
AWS reserves one IP address In each subnet's CIDR block for Route53 so you do not have enough addresses left to launch all of the new EC2 instances.
The Internet Gateway (IGW) of your VPC has scaled-up adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches.

Q10)

An AWS customer is deploying an application mat is composed of an AutoScaling group of EC2 Instances. The customers security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique x 509 certificate that contains the specific instance-id. In addition an x 509 certificates must Designed by the customer's Key management service in order to be trusted for authentication.

Which of the following configurations will support these requirements?

Configure the launched instances to generate a new certificate upon first boot Have the Key management service poll the AutoScaling group for associated instances and send new instances a certificate signature (hat contains the specific instance-id.
Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the Key management service generate a signed certificate and send it directly to the newly launched instance.
Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group Have the launched instances generate a certificate signature request with the instance's assigned instance-id to the Key management service for signature.
✅ Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure me Auto Scaling group to launch instances with this role Have the instances bootstrap get the certificate from Amazon S3 upon first boot.

Q11)

Company B is launching a new game app for mobile devices. Users will log into the game using their existing social media account to streamline data capture. Company B would like to directly save player data and scoring information from the mobile app to a DynamoDS table named Score Data When a user saves their game the progress data will be stored to the Game state S3 bucket.

What is the best approach for storing data to DynamoDB and S3?

Use an IAM user with access credentials assigned a role providing access to the Score Data DynamoDB table and the Game State S3 bucket for distribution with the mobile app.
Use Login with Amazon allowing users to sign in with an Amazon account providing the mobile app with access to the Score Data DynamoDB table and the Game State S3 bucket.
Use temporary security credentials that assume a role providing access to the Score Data DynamoDB table and the Game State S3 bucket using web identity federation.
✅ Use an EC2 Instance that is launched with an EC2 role providing access to the Score Data DynamoDB table and the GameState S3 bucket that

communicates with the mobile app via web services.

Q12) A web-startup runs its very successful social news application on Amazon EC2 with an Elastic Load Balancer, an Auto-Scaling group of Java/Tomcat application-servers, andDynamoDB as data store. The main web-application best runs on m2 x large instances since it is highly memory- bound Each new deployment requires semi-automated creationand testing of a new AMI for the application servers which takes quite a while ana is therefore only done once per week.
Recently, a new chat feature has been implemented in nodejs and wails to be integrated in the architecture. First tests show that the new component is CPU bound Because the company has some experience with using Chef, they decided to streamline the deployment process and use AWS Ops Works as an application life cycle tool to simplify management of the application and reduce the deployment cycles.
What configuration in AWS Ops Works is necessary to integrate the new chat module in the most cost-efficient and flexible way?

- Create two AWS Ops Works stacks create two AWS Ops Works layers create two custom recipe
- ✅ Create two AWS Ops Works stacks create two AWS Ops Works layers create one custom recipe
- Create one AWS Ops Works stack create two AWS Ops Works layers create one custom recipe
- Create one AWS Ops Works stack, create one AWS Ops Works layer, create one custom recipe

Q13)

You are implementing a URL whitelisting system for a company that wants to restrict outbound HTTP'S connections to specific domains from their EC2-hosted applications you deploy a single EC2 instance running proxy software and configure It to accept traffic from all subnets and EC2 instances in the VPC. You configure the proxy to only pass through traffic to domains that you define in its whitelist configuration You have a nightly maintenance window or 10 minutes where ail instances fetch new software updates. Each update Is about 200MB In size and there are 500 instances In the VPC that routinely fetch updates After a few days you notice that some machines are failing to successfully download some, but not all of their updates within the maintenance window. The download URLs used for these updates are correctly listed in the proxy's whitelist configuration and you are able to access them manually using a web browser on the instances.

What might be happening? (Choose 2 answers)

- The route table for the subnets containing the affected EC2 instances is not configured to direct network traffic for the software update locations to the proxy.
- You are running the proxy on a affilelentiy-sized EC2 instance in a private subnet and its network throughput is being throttled by a NAT running on an undersized EO£ instance
- ✅ You are running the proxy in a public subnet but have not allocated enough EIPs lo support the needed network throughput through the Internet Gateway (IGW)
- ✅ You have not allocated enough storage to the EC2 instance running me proxy so the network buffer is filling up. causing some requests to fall
- You are running the proxy on an undersized EC2 instance type so network throughput is not sufficient for all instances to download their updates in time.

Q14) Your fortune 500 company has under taken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware The outcome was that ail employees would be granted access to use Amazon S3 for storage of their personal documents. Which of the following will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket? (Choose 3 Answers)

- Configuring IAM role
- ✅ Tagging each folder in the bucket
- ✅ Using AWS Security Token Service to generate temporary tokens
- ✅ Setting up a federation proxy or identity provider
- Setting up a matching IAM user for every user in your corporate directory that needs

Q15) To serve Web traffic for a popular product your chief financial officer and IT director have purchased 10 ml large heavy utilization Reserved Instances (RIs) evenly spread across two availability zones: Route 53 is used to deliver the traffic to an Elastic Load Balancer (ELB). After several months, the product grows even more popular and you need additional capacity As a result, your company purchases two C3.2xlarge medium utilization Ris You register the two c3 2xlarge instances with your ELB and quickly find that the ml large instances are at 100% of capacity and the c3 2xlarge instances have significant capacity that's unused Which option is the most cost effective and uses EC2 capacity mosteffectively?

- ✅ Configure ELB with two c3 2xiarge Instances and use on-demand Autoscailng group for up to two additional c3.2xlarge instances Shut on mi .large instances.
- Route traffic to EC2 ml large and c3 2xlarge instances directly using Route 53 latency based routing and health checks shut off ELB
- Use a separate ELB for each instance type and distribute load to ELBs with Route 53 weighted round robin
- Configure Autoscaning group and Launch Configuration with ELB to add up to 10 more on-demand mi large instances when triggered by Cloudwatch shut off c3 2xiarge instances

Q16)

A web design company currently runs several FTP servers that their 250 customers use to upload and download large graphic files They wish to move this system to AWS to make it more scalable, but they wish to maintain customer privacy and Keep costs to a minimum.

What AWS architecture would you recommend?

- Create a single S3 bucket with Requester Pays turned on and ask their customers to use an S3 client instead of an FTP client Create a bucket tor each customer with a Bucket Policy that permits access only to that one customer.
- ✅ Create an auto-scaling group of FTP servers with a scaling policy to automatically scalein when minimum network traffic on the auto-scaling group is below a given threshold. Load a central list of ftp users from S3 as part of the user Data startup script on each Instance.
- Create a single S3 bucket with Reduced Redundancy Storage turned on and ask their customers to use an S3 client instead of an FTP client Create a bucket for each customer with a Bucket Policy that permits access only to that one customer.
- ASK their customers to use an S3 client instead of an FTP client. Create a single S3 bucket Create an IAM user for each customer Put the IAM Users in a Group that has an IAM policy that permits access to sub-directories within the bucket via use of the 'username' Policy variable

Q17)

You are running a news website in the eu-west-1 region that updates every 15 minutes. The website has a world-wide audience it uses an Auto Scaling group behind an Elastic Load Balancer and an Amazon RDS database Static content resides on Amazon S3, and is distributed through Amazon CloudFront. Your Auto Scaling group is set to trigger a scale up event at 60% CPU utilization, you use an Amazon RDS extra large DB instance with 10.000 Provisioned IOPS its CPU utilization is around 80%. While freeable memory is in

the 2 GB range. Web analytics reports show that the average load time of your web pages is around 1 5 to 2 seconds, but your SEO consultant wants to bring down the average load time to under 0.5 seconds.

How would you improve page load times for your users? (Choose 3 answers)

- Set up a second installation in another region, and use the Amazon Route 53 latencybased routing feature to select the right region.
- ✓ Switch Amazon RDS database to the high memory extra large Instance type
- Configure Amazon CloudFront dynamic content support to enable caching of re-usable content from your site
- ✓ Add an Amazon ElastiCache caching layer to your application for storing sessions and frequent DB queries
- ✓ Lower the scale up trigger of your Auto Scaling group to 30% so it scales more aggressively

---

Q18)

You have been asked to design the storage layer for an application. The application requires disk performance of at least 100,000 IOPS in addition, the storage layer must be able to survive the loss of an individual disk. EC2 instance, or Availability Zone without any data loss. The volume you provide must have a capacity of at least 3 TB.

Which of the following designs will meet these objectives'?

- Instantiate a c3 8xlarge Instance in us-east-1 Provision 3x1TB EBS volumes attach them to the instance, and configure them as a single RAID 0 volume Ensure that EBS snapshots are performed every 15 minutes.
- ✓ Instantiate a c3 8xlarge instance in us-east-i provision 4x1TB EBS volumes, attach them to the instance, and configure them as a single RAID 5 volume Ensure that EBS snapshots are performed every 15 minutes.
- Instantiate a c3 8xlarge Instance In us-east-1 Provision an AWS Storage Gateway and configure it for 3 TB of storage and 100 000 IOPS Attach the volume to the instance.
- Instantiate an 12 8xlarge instance in us-east-1a create a raid 0 volume using the four 800GB SSD ephemeral disks provide with the Instance Configure synchronous block-level replication to an Identically configured Instance in us-east-1b.
- Instantiate an 12 8xlarge instance in us-east-1a Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance Provision 3x1 TB EBS volumes attach them to the instance and configure them as a second RAID 0 volume Configure synchronous, block-level replication from the ephemeral-backed volume to the EBS-backed volume.

Q19)

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC Your server's on-premises will de-communicating with your VPC instances.

You will de-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)

- ✓ 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

Q20) What is a requirement for attaching EC2 instances to on-premises clients and applications?

- VPN Connection
- ✓ Amazon Internet Gateway

Explanation:-An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. Refer: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

- Amazon Virtual Private Gateway (VPN)
- Elastic Load Balancer (ELB)
- NAT

Q21) What two statements correctly describe Amazon virtual private gateway?

- Single virtual private gateway per region
- Multiple virtual private gateways per VPC
- ✓ Single virtual private gateway per VPC
- Assign to public subnets only
- ✓ Assign to private subnets only

Q22) What is the maximum access port speed available with Amazon Direct Connect service?

- 500 Mbps
- ✓ 10 Gbps

Explanation:-AWS Direct Connect makes it easy to scale your connection to meet your needs. AWS Direct Connect provides 1 Gbps and 10 Gbps connections, and you can easily provision multiple connections if you need more capacity. Refer: https://aws.amazon.com/directconnect/#:~:text=AWS%20Direct%20Connect%20makes%20it,if%20you%20need%20more%20capacity.

- 1 Gbps
- 100 Gbps
- 100 Mbps

Q23)

Your company plans to host a large donation website on Amazon Web Services (AWS). You anticipate a large and undetermined amount of traffic that will create many database writes. To be certain that you do not drop any writes to a database hosted on AWS.

Which service should you use?

- Amazon DynamoDB with provisioned write throughput up to the anticipated peak write

- Amazon ElastiCache to store the writes until the writes are committed to the database.
- Amazon Simple Queue Service (SOS) for capturing the writes and draining the queue to write to the database.
- ✓ Amazon RDS with provisioned IOPS up to the anticipated peak write throughput.

Q24) What are three recommended best practices when configuring Identity and Access Management (IAM) security services?

- ✓ share your password and/or access keys with members of your group only

Explanation:-Refer: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

- IAM groups are not recommended for storage security
- ✓ Create an IAM user with administrator privileges
- ✓ Lock or delete your root access keys when not required
- Remove unnecessary credentials

Q25) What two features create security zones between EC2 instances within a VPC?

- Network ACL
- Virtual Security Gateway
- ✓ Security groups
- ✓ WAF

Q26) What AWS service provides vulnerability assessment services to tenants within the cloud?

- ✓ Amazon Trusted Advisor
- Amazon Cloud Logic
- Amazon Inspector
- Amazon WAF

Q27) What are two primary differences between AD Connector and Simple AD for cloud directory services?

- Simple AD provides enhanced integration with IAM
- Simple AD is more scalable than AD Connector
- ✓ AD Connector requires an on-premises ADS directory
- Simple AD is fully managed and setup in minutes
- ✓ Simple AD requires an on-premises ADS directory

Q28)

Your team has a tomcat-based Java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC.

Which of the following optimal setup for persistence and security meets the above requirements?

- Create your RDS instance separately and pass its DNS name to your's DB connection string as an environment variable Alter its security group to allow access to It from hosts In your application subnets.
- Create your RDS instance separately and add its IP address to your application's DB connection strings in your code Alter its security group to allow access to it from hosts within your VPC's IP address block.
- Create your RDS instance separately and pass its DNS name to your app's DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself.
- ✓ Create your RDS instance as part of your Elastic Beanstalk definition and alter its security group to allow access to it from hosts in your application subnets.

Q29)

Your firm has uploaded a large amount of aerial image data to S3 In the past, in your onpremises environment, you used a dedicated group of servers to oaten process this data and used Rabbit MQ - An open source messaging system to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your managertold you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost.

Which of the following option is correct?

- ✓ Use SNS to pass job messages use Cloud Watch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.
- Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SOS Once data is processed,
- Change the storage class of the S3 objects to Reduced Redundancy Storage. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS Once data is processed, change the storage class of the S3 objects to Glacier
- Use SQS for passing job messages use Cloud Watch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.

Q30) Out of the stripping options available for the EBS volumes, which one has the following disadvantage : 'Doubles the amount of I/O required from the instance to EBS compared to RAID 0, because you're mirroring all writes to a pair of volumes, limiting how much you can stripe.' ?

- Raid 1
- ✓ RAID 1+0 (RAID 10)
- Raid 0
- Raid

Q31) Where are HTMLfiles sourced from when they are not cached at a CloudFront edge location?

- RTMP server
- Nearest edge location

S3 bucket
origin HTTP server
Explanation:-CloudFront compares the request with the specifications in your distribution and forwards the request for the files to your origin server for the corresponding file type—for example, to your Amazon S3 bucket for image files and to your HTTP server for HTML files. Refer: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HowCloudFrontWorks.html
S3 object
Failover edge location

Q32) What is the capacity of a single Kinesis shard?

10 MB/sec data input and 10 MB/sec data output
1 MB/sec data input and 2 MB/sec data output
Explanation:-Shard is the base throughput unit of a Kinesis stream. One shard provides a capacity of 1MB/sec data input and 2MB/sec data output. One shard can support up to 1000 PUT records per second. You will specify the number of shards needed when you create a stream. Refer: https://www.amazonaws.cn/en/kinesis/data-streams/faqs/#:~:text=Shard%20is%20the%20base%20throughput,when%20you%20create%20a%20stream.
2000 PUT records per second
1000 PUT records per second
Unlimited

Q33) What Amazon AWS service supports real-time processing of data stream from multiple consumers and replay of records?

SQS
Kinesis data streams
Explanation:-Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. Refer: https://aws.amazon.com/kinesis/data-streams/faqs/#:~:text=Amazon%20Kinesis%20Data%20Streams%20enables%20real%2Dtime%20processing%20of%20streaming,to%20multiple%20Amazon%20Kinesis%20Applicati
EMR
DynamoDB
RedShift

Q34) What AWS service is used to monitor tenant remote access and various security errors including authentication retries?

CloudWatch
CloudFront
Telnet
SSH

Q35) How does Amazon AWS isolate metrics from different applications for monitoring, store and reporting purposes?

Beanstalk
CloudTrail
namespaces
Explanation:-Container Insights provides automatic dashboards in the CloudWatch console. These dashboards summarize the compute performance, errors, and alarms by cluster, pod/task, and service. For Amazon EKS and k8s, dashboards are also available for nodes/EC2 instances and namespaces. Each dashboard summarizes the list of running pods/tasks or containers by CPU and memory for the selected time window, and allows you to contextually - based on time window and selected pod/task or container - dive deeper into application logs, AWS X-Ray traces, and performance events. You can always retrieve metrics data for any Amazon EC2 instance based on the retention schedules described above. However, the CloudWatch console limits the search of metrics to 2 weeks after a metric is last ingested to ensure that the most up to date instances are shown in your namespace. Refer: https://aws.amazon.com/cloudwatch/features/
EC2 instances
Docker

Q36) What Amazon AWS service provides account transaction monitoring and security audit?

CloudWatch
CloudTrail
Explanation:-AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Refer: https://aws.amazon.com/cloudtrail/#:~:text=AWS%20CloudTrail%20is%20a%20service,actions%20across%20your%20AWS%20infrastructure.
CloudFront
Security group

Q37) What two statements correctly describe CloudWatch monitoring of database instances?

RDS does not support monitoring of operating system metrics
Metrics are not enabled automatically for DynamoDB and RDS
Alarms must be configured for DynamoDB and RDS within CloudWatch
Metrics are sent automatically from DynamoDB and RDS to CloudWatch

---

Q38) What AWS service can send notifications to customer smartphones and mobile applications with attached video and/or alerts?

SQS
SNS
Explanation:-With Amazon SNS , you have the ability to send push notification messages directly to apps on mobile devices. Push notification messages sent to a mobile endpoint can appear in the mobile app as message alerts, badge updates, or even sound alerts. Refer: https://docs.aws.amazon.com/sns/latest/dg/sns-mobile-application-as-subscriber.html#:~:text=With%20Amazon%20SNS%20%2C%20you%20have,updates%2C%20or%20even%20sound%20alerts.
Lambda
EMR
CloudTrail

Q39) What is required to prevent an instance from being launched and incurring costs?

- Stop instance
- Terminate instance
- Terminate AMI and de-register instance
- Stop and de-register instance
- ✅ Stop, deregister AMI and terminate instance

Explanation:-You can delete your instance when you no longer need it. This is referred to as terminating your instance. As soon as the state of an instance changes to shutting-down or terminated, you stop incurring charges for that instance.

You can't connect to or start an instance after you've terminated it. However, you can launch additional instances using the same AMI.

Refer: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

---

Q40) What is an EBS Snapshot?

- Backup of configuration settings
- Backup of an EC2 instance
- ✅ Backup of an EBS root volume and instance data

Explanation:-An EBS snapshot is a point-in-time copy of your Amazon EBS volume, which is lazily copied to Amazon Simple Storage Service (Amazon S3). EBS snapshots are incremental copies of data. This means that only unique blocks of EBS volume data that have changed since the last EBS snapshot are stored in the next EBS snapshot. Refer: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

- Backup of instance store

Q41) Where are Elastic Load Balancer and Auto-Scaling groups deployed as a unified solution for horizontal scaling?

- ✅ Web server instances
- All instances

Explanation:-When you create an Auto Scaling group, you must specify the necessary information to configure the Amazon EC2 instances, the subnets for the instances, and the initial number of instances.

To configure Amazon EC2 instances, you can specify a launch configuration, a launch template, or an EC2 instance. The following procedure demonstrates how to create an Auto Scaling group using an EC2 instance. To use a launch configuration or a launch template, see Creating an Auto Scaling Group Using a Launch Configuration or Creating an Auto Scaling Group Using a Launch Template.

Refer: https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-from-instance.html

When you create an Auto Scaling group using an EC2 instance, Amazon EC2 Auto Scaling creates a launch configuration for you and associates it with the Auto Scaling group. This launch configuration has the same name as the Auto Scaling group, and it derives its attributes from the specified instance, such as AMI ID, instance type, and Availability Zone. Refer: This is the new world of scalable, on-demand web services. Pay for what you need and use, and not a byte more. Shortly after the launch of Amazon Elastic Compute Cloud (EC2), it was easy to do this with the simultaneous launch of Elastic Load Balancing, EC2 Auto Scaling, and Amazon CloudWatch. Since then we have added Auto Scaling to other AWS services including ECS, Spot Fleets, DynamoDB, Aurora, AppStream 2.0, and EMR. We have also added features such as target tracking to make it easier for you to scale based on the metric that is most appropriate for your application. Refer: https://aws.amazon.com/blogs/aws/aws-auto-scaling-unified-scaling-for-your-cloud-applications/

- Database instances
- Default VPC only

Q42) What feature is supported when attaching or detaching an EBS volume from an EC2 instance?

- ✅ EBS volume can only be attached and detached to an EC2 instance in the same Availability Zone

Explanation:-You can attach an available EBS volume to one or more of your instances that is in the same Availability Zone as the volume. Refer: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-attaching-volume.html

- EBS volume can be attached and detached to an EC2 instance in the same region
- EBS volume can be attached and detached to an EC2 instance that is cross-region
- EBS volume can only be copied and attached to an EC2 instance that is cross-region

---

Q43) How is DNS Route 53 configured for Multi-Site fault tolerance? (Select two)

- Zero weighted records
- Alias records
- ✅ Health checks
- ✅ Weighted records (non-zero)
- IP address

Q44) What is an Availability Zone?

- Single region
- Multiple regions
- Multiple VPCs
- ✅ Data center

Explanation:-An Availability Zone is a high-availability offering that protects your applications and data from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. Refer: https://docs.microsoft.com/en-us/azure/availability-zones/az-overview

- Multiple EC2 server instances

Q45) How are DNS records managed with Amazon AWS to enable high availability?

- Elastic load balancing
- ✅ Reverse proxy

Explanation:-From split-horizon DNS to customer domain-based DNS records for AWS PrivateLink endpoints, enable varying degrees of traffic rerouting and high availability with ownership/management of the DNS infrastructure. Any implementation must consider a trade-off between service availability, changes to the client application, and management of DNS infrastructure. Refer: https://aws.amazon.com/blogs/apn/reviewing-dns-mechanisms-for-routing-traffic-and-enabling-failover-for-aws-privatelink-deployments/

- Server health checks
- Auto-Scaling

Q46) What two statements correctly describe how to add or modify IAM roles to a running EC2 instance?

- Attach an IAM role to the user account and relaunch the EC2 instance
- ✅ Replace an IAM role attached to an existing EC2 instance from the EC2 console

Explanation:-To replace the IAM role on an instance that already has an attached IAM role, the instance must be in the running state. You can do this if you want to change the IAM role for an instance without detaching the existing one first. For example, you can do this to ensure that API actions performed by applications running on the instance are not interrupted.

To replace an IAM role for an instance (console)

Open the Amazon EC2 console at https://console.amazonaws.cn/ec2/.

In the navigation pane, choose Instances.

Select the instance, choose Actions, Instance Settings, Attach/Replace IAM role.

Select the IAM role to attach to your instance, and choose Apply.

Refer: https://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

- ✅ Attach an IAM role to an existing EC2 instance from the EC2 console

Explanation:-Attaching an IAM role to an instance

To attach an IAM role to an instance that has no role, the instance can be in the stopped or running state.

To attach an IAM role to an instance (console)

Open the Amazon EC2 console at https://console.amazonaws.cn/ec2/.

In the navigation pane, choose Instances.

Select the instance, choose Actions, Instance Settings, Attach/Replace IAM role.

Select the IAM role to attach to your instance, and choose Apply.

Refer: https://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

- Add the EC2 instance to a group where the role is a member

Q47) What is the default behavior for an EC2 instance when terminated? (Select two)

- ✅ EBS root device volume is automatically deleted when instance terminates
- ✅ EBS data volumes that you attach at launch persist
- EBS root device volume and additional attached volumes are deleted immediately

Explanation:-If EC2 instance is terminated, by default the root volume is also deleted. But the EBS volume attached will be retained. We can change this default behavior by modifying the DeleteOnTermination attribute. When an instance terminates, the data on any instance store volumes associated with that instance is deleted. By default, Amazon EBS root device volumes are automatically deleted when the instance terminates. Refer: When an instance terminates, the data on any instance store volumes associated with that instance is deleted. By default, Amazon EBS root device volumes are automatically deleted when the instance terminates.

- DeleteOnTermination attribute cannot be modified

Q48) How do you launch an EC2 instance after it is terminated? (Select two)

- Reboot instance from management console
- ✅ Launch a new instance from a Snapshot
- Reboot instance from CLI
- ✅ Launch a new instance using the same AMI

Explanation:-You can't connect to or start an instance after you've terminated it. However, you can launch additional instances using the same AMI. If you'd rather stop and start your instance, or hibernate it, see Stop and start your instance or Hibernate your Linux instance. Refer: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html#:~:text=You%20can't%20connect%20to,or%20Hibernate%20your%20Linux%20instance.

- Contact AWS support to reset

Q49) What service can automate EBS snapshots (backups) for restoring EBS volumes?

- Amazon Inspector
- CloudTrail
- SNS topic
- ✅ CloudWatch event

Explanation:-CloudWatch metrics are statistical data that you can use to view, analyze, and set alarms on the operational behavior of your volumes.

You can use Amazon Data Lifecycle Manager to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes. Automating snapshot management helps you to:

Protect valuable data by enforcing a regular backup schedule.

Retain backups as required by auditors or internal compliance.

Reduce storage costs by deleting outdated backups.

Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon Data Lifecycle Manager provides a complete backup solution for EBS volumes at no additional cost.

Refer:

- CloudWatch alarm

Q50) What will cause AWS to terminate an EC2 instance on launch? (Select two)

- multiple IP addresses assigned to instance
- ✅ EBS volume limits exceeded
- ✅ number of EC2 instances on AWS account exceeded
- security group error
- unsupported instance type assigned

Q51)

You recently made some configuration changes to an EC2 instance. You then launched a new EC2 instance from the same AMI however none of the settings were saved.

What is the cause of this error?

- did not reboot EC2 instance to enable changes
- ✅ did not create new AMI
- did not save configuration changes to AMI
- did not save configuration changes to EC2 instance

Q52) What statements are correct concerning DisableApiTermination attribute? (Select two)

- DisableApiTermination attribute supported for EBS-backed instances only
- Can enable termination protection for Spot instances
- Termination protection is enabled by default for an EC2 instance
- ✅ Termination protection is disabled by default for an EC2 instance
- ✅ Cannot enable termination protection for Spot instances

Explanation:-The DisableApiTermination attribute controls whether the instance can be terminated using the console, CLI, or API. By default, termination protection is disabled for your instance. Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

---

Q53) What is required to copy an encrypted EBS snapshot cross-account? (Select two)

- Share the encrypted EBS snapshots publicly
- ✅ Share the encrypted EBS snapshot with the target account
- ✅ Share the custom key for the snapshot with the target account

Explanation:-Cross-Account Copying

To create a copy of the encrypted EBS snapshot in another account you need to complete four simple steps:

1. Share the custom key associated with the snapshot with the target account.

2. Share the encrypted EBS snapshot with the target account.

3. In the context of the target account, locate the shared snapshot and make a copy of it.

4. Use the newly created copy to create a new volume.

Refer: https://aws.amazon.com/blogs/aws/new-cross-account-copying-of-encrypted-ebs-snapshots/#:~:text=To%20create%20a%20copy%20of,snapshot%20with%20the%20target%20account.&text=In%20the%20context%20of%20the,to%20create%20a%20new%20volu

- Distribute the custom key from CloudFront
- Copy the unencrypted EBS snapshot to an S3 bucket
- Enable root access security on both accounts

Q54) What three services enable Single-AZ as a default?

- ✅ Auto-Scaling
- ✅ ELB
- ✅ EC2
- DynamoDB
- S3

Q55) How is an Amazon Elastic Load Balancer (ELB) assigned?

- Per subnet
- Per Auto-Scaling group
- ✅ Per EC2 instance
- Per VPC

Q56) What method detects when to replace an EC2 instance that is assigned to an Auto-Scaling group?

- not currently supported
- EC2 health check
- load balancing algorithm
- ✅ health check

Explanation:-A Classic Load Balancer is recommended only for EC2 Classic instances. The Application Load Balancer operates at the request level only. If you're dealing with HTTP requests, which you are for your web application, you can use this. It supports the basic feature of distributing requests using the round robin algorithm.

- dynamic path detection
- Auto-Scaling

Q57) What two statements correctly describe Auto-Scaling groups?

- Database instances only
- ✅ EC2 instances are assigned to a group
- Decrease number of instances only
- ✅ Horizontal scaling of capacity

Explanation:-An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service. Refer: https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html

- No support for multiple availability zones

Q58) What is the default maximum number of Elastic IP addresses assignable per Amazon AWS region?

✅ 5

Explanation:-By default, all AWS accounts are limited to five (5) Elastic IP addresses per Region, because public (IPv4) internet addresses are a scarce public resource. Refer: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/elastic-ip-addresses-eip.html#:~:text=Sending%20Limitations%20page.-,Elastic%20IP%20address%20limit,are%20a%20scarce%20public%20resource.

- 100
- 1
- unlimited