Answer Sheet

Q1)

Your customer is willing to consolidate their log streams, access logs, application logs, security logs etc. in one single system. Once consolidated, the customer wants to analyze these logs in real time based on heuristics.

From time to time, the customer needs to validate heuristics, which requires going back to data samples extracted from the last 12 hours?

What is the best approach to meet your customer's requirements?

- Setup Auto Scaling group of EC2 syslogd servers, store the logs S3 use EMR to apply heuristics on the logs
- Configure Amazon Cloud Trail to receive custom logs, use EMR to apply heuristics the logs
- ✅ Send all the log events to Amazon Kinesis. Develop a client process to apply heuristics on the logs

Explanation:-Whenever the scenario - just like this one - wants to do real-time processing of a stream of data, always think about Amazon Kinesis. Also, remember that the records of the stream is available for 24 hours. Option A is incorrect because SQS is not used for real time processing of stream of data. Option B is CORRECT because Amazon Kinesis is best suited for application that does the real-time processing of stream of data. Also, the records of the stream is available for 24 hours in Kinesis. Option C is incorrect because CloudTrail is not used to process the real-time data processing and EMR is used for batch-processing. Option D is incorrect because setting autoscaling of EC2 instances is not cost-effective and EMR is used for batch-processing. More information on Amazon Kinesis: Amazon Kinesis is a platform for streaming data on AWS, making it easy to load and analyze streaming data, and also providing the ability for you to build custom streaming data applications for specialized needs. Use Amazon Kinesis Streams to collect and process large streams of data records in real time. Use Amazon Kinesis Firehose to deliver real-time streaming data to destinations such as Amazon S3 and Amazon Redshift. Use Amazon Kinesis Analytics to process and analyze streaming data with standard SQL. For more information on Kinesis, please visit the below URL: https://aws.amazon.com/documentation/kinesis/ The correct answer is: Send all the log events to Amazon Kinesis. Develop a client process to apply heuristics on the logs

- Send all the log events to Amazon SQS. Setup an Auto Scaling group of EC2 servers to consume the logs and apply the heuristics.

Q2)

An administrator is using Amazon CloudFormation to deploy a three-tier web application that consists of a web tier and application tier that will utilize Amazon DynamoDB for storage.

While creating the CloudFormation template which of the following would allow the application instance access to the DynamoDB tables without exposing API credentials?

- Use the Parameter section in the Cloud Formation template to have the user input Access and Secret Keys from an already created IAM user that has me permissions required to read and write from the required DynamoDB table.
- Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and associate the Role to the application instances by referencing an instance profile.
- ✅ Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and reference the Role in the instance profile property of the application instance.

Explanation:-The scenario requires the instance to have access to DynamoDB tables without having to use the API credentials. In such scenarios, always think of creating IAM Roles rather than IAM Users. Option A is incorrect because the IAM Role is not associated to the application by referencing an instance profile, it has to be used as an instance profile property. Option B is incorrect because (a) you should never expose the Access and Secret Keys while accessing the AWS resources, and (b) using IAM Role is more secured way of accessing the resources than using IAM Users with security credentials. Option C is CORRECT because (a) it uses IAM Role with the appropriate permissions to access the resource, and (b) it references that Role in the instance profile property of the application instance. See an example given below: Option D is incorrect because (a) you should never expose the Access and Secret Keys while accessing the AWS resources, (b) using IAM Role is more secured way of accessing the resources than using IAM Users with security credentials. For more information on granting access to AWS resources via EC2 instance profile property, please visit the below URL: https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/java-dg-roles.html For more information on adding IAM roles in CloudFormation templates, please visit the below URL: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-iam-role.html The correct answer is: Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and reference the Role in the instance profile property of the application instance.

- Create an identity and Access Management user in the CloudFormation template that has permissions to read and write from the required DynamoDB table, use the GetAtt function to retrieve the Access and secret keys and pass them to the application instance through user-data.

Q3)

Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high-resolution MP4 format.

Your workforce is distributed globally often on the move and using company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video.

Your company has no video transcoding expertise and it required that you may need to pay for a consultant.

How do you implement the most cost-efficient architecture without compromising high availability and quality of video delivery'?

- Elastic Transcoder to transcode original nigh-resolution MP4 videos to HLS EBS volumes to host videos and EBS snapshots to incrementally backup original rues after a few days. CloudFront to serve HLS transcoded videos from EC2.
- A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days CloudFront to serve HLS transcoded videos from EC2
- A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number or nodes depending on the length of the queue. Use S3 to host videos with Lifecycle Management to archive all files to Glacier after a few days. Use CloudFront to serve HLS transcoding videos from Glacier
- ✅ Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. Use S3 to host videos with Lifecycle Management to archive original flies to Glacier after a few days. Use CloudFront to serve HLS transcoded videos from S3.

Explanation:-There are four most important design considerations here: (a) video transcoding expertise, (b) global distribution of the content, (c) cost-effective solution, and (d) no compromise with the high availability and quality of the video delivery. Amazon Elastic Transcoder is a media transcoding service in the cloud. It is designed to be a highly scalable, easy to use and a cost-effective way for developers and businesses to convert (or "transcode") media files from their source format into versions that will playback on various devices like smartphones, tablets, and PCs. Option A is CORRECT because (a) it uses Amazon Elastic Transcoder that converts from MP4 to HLS, (b) S3 Object Lifecycle Management reduces the cost by archiving the files to Glacier, and (c) CloudFront - which is a highly available service - enables the global delivery of the video without compromising the video delivery speed or quality. Option B is incorrect because (a) it necessitates the overhead of infrastructure provisioning. i.e deploying of EC2 instances, auto scaling, SQS queue / pipeline, (b) setting up of EC2 instances to handle global delivery of content is not a cost efficient solution. Option C is incorrect because the use of EBS snapshots is not a cost effective solution compared to S3 Object Lifecycle Management. Option D is incorrect because (a) it necessitates the overhead of infrastructure provisioning. i.e deploying of EC2 instances, auto scaling, SQS queue / pipeline, (b) setting up of EC2 instances to handle global delivery of content is not a cost efficient solution, and (d) the use of EBS snapshots is not a cost effective solution compared to S3 Object Lifecycle Management. For more information on Elastic Transcoder, please visit the below URL: https://aws.amazon.com/elastictranscoder/ CloudFront can be then used to deliver the content to the users from its various edge locations. The correct answer is: Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. Use S3 to host videos with Lifecycle Management to archive original flies to Glacier after a few days. Use CloudFront to serve HLS transcoded videos from S3.

Q4)

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, and DynamoDB as a data store. The main web application best runs on m2 x large instances since it is highly memory- bound.

Each new deployment requires the semi-automated creation and testing of a new AMI for the application servers which takes quite a while and is therefore only done once per week. Recently, a new chat feature has been implemented in Node.js and waits to be integrated into 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 lifecycle 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 one AWS Ops Works stack, create one AWS Ops Works layer, create one 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

Explanation:-The scenario here requires that you need to manage the application that is created with java, node.js, and DynamoDB using AWS OpsWork. The deployment process should be streamlined and the deployment cycles should be reduced. As the java and node.js have different resource requirements, it makes sense to deploy them on different layers. It would make the maintenance easier as well. Option A is incorrect because it would be a better solution to create two separate layers: one for Java and one for node.js. Option B is CORRECT because only one stack would be sufficient, and two layers (one for Java and one for node.js) would be required for handling separate requirements. One custom recipe for DynamoDB would be required. Option C is incorrect because two OpsWork stacks are unnecessary. Option D is incorrect because two OpsWork stacks are unnecessary. More information on AWS OpsWork Stack An AWS OpsWorks Stack defines the configuration of your entire application: the load balancers, server software, database, etc. You control every part of the stack by building layers that define the software packages deployed to your instances and other configuration details such as Elastic IPs and security groups. You can also deploy your software onto layers by identifying the repository and optionally using Chef Recipes to automate everything Chef can do, such as creating directories and users, configuring databases, etc. You can use OpsWorks Stacks' built-in automation to scale your application and automatically recover from instance failures. You can control who can view and manage the resources that are used by your application, including ssh access to the instances that your application uses. For more information on Ops work, please visit the below URL https://aws.amazon.com/opsworks/stacks/faqs/ The correct answer is: Create one AWS Ops Works stack create two AWS Ops Works layers, create one custom recipe

- Create two AWS Ops Works stacks create two AWS Ops Works layers, create two custom recipe

---

Q5)

A company wants to train a group of people on AWS. They have divided the groups into 3 teams.

They want each team to have their own environment to experiment with the AWS resources.

Which of the below options will help fulfill the above requirement?

- Create separate IAM users and VPCs and allow each IAM user to have access to separate VPCs.
- ✅ Create a VPC with subnets and allow access to each subnet for each team.
- Create separate AWS accounts for each team.
- Create an IAM user for each team and allow them permission to launch certain services.

Q6)

A legacy application needs to be moved to AWS. But the legacy application has a dependency on multicast?

Which of the below options need to be considered to ensure the legacy application works in the AWS environment?

- Create all the subnets on a different VPC and use VPC peering between them.
- All of the answers listed will help in deploying applications that require multicast on AWS.
- Provide Elastic Network Interfaces between the subnets.
- ✅ Create a virtual overlay network that runs on the OS level of the instance.

Q7)

A web company is looking to implement an intrusion detection and prevention system for their deployed VPC.

This platform should have the ability to scale to thousands of instances running inside of the VPC.

How should they architect their solution to achieve these goals?

Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.
Configure servers running in the VPC using the host-based 'route' commands to send all traffic through the platform to a scalable virtualized IDS/IPS.
Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see all traffic across the VPC.
✅ Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides

Explanation:-This quesion is asking you to design a scalable IDS/IPS solution (easily applicable to thousands of instances). There are couple of ways of designing the IDS/IPS systems: (1) install the IDS/IPS agents on each instance in the VPC, and (2) create a separate Security-VPC with only IDS/IPS instances, and route the incoming traffic via this VPC to the other VPC that contains the other EC2 resources. Option A is incorrect because promiscous mode is not supported by AWS. Option B is CORRECT because it creates a second VPC which contains the scalable IDS/IPS resources, and routes the trafic via these VPC to other VPC. Option C is incorrect because the traffic should flow FROM the security VPC, not TO it. Option D is plausible, but (a) it is not a scalable solution, (b) it is only IDS solution, not IPS solution. Please find the below URL to a good slide deck from AWS for getting IDS in place. https://awsmedia.s3.amazonaws.com/SEC402.pdf The correct answer is: Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides

---

Q8)

A large real-estate brokerage is exploring the option of adding a cost-effective location-based alert to their existing mobile application. The application backend infrastructure currently runs on AWS.

Users who opt into this service will receive alerts on their mobile device regarding real-estate offers in proximity to their location.

For the alerts to be relevant, delivery time needs to be in the low minute count.

The existing mobile app has 5 million users across the US.

Which one of the following architectural suggestions would you make to the customer?

The mobile application will submit its location to a web service endpoint utilizing Elastic Load Balancing and EC2 instances. DynamoDB will be used to store and retrieve relevant offers from EC2 instances which will then communicate with mobile earners/device providers to push alerts back to mobile application.
✅ The mobile application will send device location using SQS. EC2 instances will retrieve the relevant offers from DynamoDB. AWS Mobile Push will be used to send offers to the mobile application

Explanation:-The scenario has following architectural considerations: (1) the users should get notifications about the real estate in the area near to their location, (2) only subscribed users should get the notification, (3) the notification delivery should be fast, (4) the architecture should be scalable, and (5) it should be cost effective. When the question has considerations for scalability, always think about DynamoDB as it is the most recommended database solution to handle huge amount of data/records. For automated notifications, always think about SNS. Option A is incorrect because (a) setting up EC2 instances and ELB to handle 5 millions users will not be cost effective, and (b) sending the notifications via mobile earners/device providers as alerts is neither feasible nor cost effective (certainly not as cost effective as SNS). Option B is incorrect because (a) setting up EC2 instances and ELB to handle 5 millions users will not be cost effective, (b) receiving location via Direct Connect and carrier connection is not cost effective, also it does not deal with subscriptions, and (c) sending the notifications via mobile carriers as alerts is not cost effective (certainly not as cost effective as SNS). Option C is CORRECT because (a) SQS is a highly scalable, cost effective solution for carrying out utility tasks such as holding the location of millions of users, (b) it uses highly scalable DynamoDB, and (c) it uses the cost effective AWS SNS Mobile Push service to send push notification messages directly to apps on mobile devices. Option D is incorrect because AWS SNS Mobile Push service to used for sending push notification messages to the mobile devices, not to get the location of the mobile devices. For more information on AWS SNS Mobile Push, please see the diagram and link given below: https://docs.aws.amazon.com/sns/latest/dg/SNSMobilePush.html The correct answer is: The mobile application will send device location using SQS. EC2 instances will retrieve the relevant offers from DynamoDB. AWS Mobile Push will be used to send offers to the mobile application
The mobile application will send device location using AWS Mobile Push. EC2 instances will retrieve the relevant offers from DynamoDB. EC2 instances will communicate with mobile carriers/device providers to push alerts back to the mobile application.
Use AWS DirectConnect or VPN to establish connectivity with mobile carriers EC2 instances will receive the mobile applications 'location through carrier connection. RDS will be used to store and relevant offers. EC2 instances will communicate with mobile carriers to push alerts back to the mobile application

---

Q9)

There is a requirement to host a database server. This server should not be able to connect to the internet except in the case of downloading the required database patches.

Which of the following solutions would be the best to satisfy all the above requirements? Choose the correct answer from the below options.

Set up the database in a private subnet with a security group which only allows outbound traffic.
Set up the database in a public subnet with a security group which only allows inbound traffic.
✅ Set up the database in a private subnet which connects to the Internet via a NAT instance.

Explanation:-You should set up the data server in private subnet as it needs only the traffic from NAT instance or NAT Gateway, and not from the internet.

Set up the database in a local data center and use a private gateway to connect the application to the database.

Q10) Which of the below options is the most suited for connecting your on-premise Active Directory services to AWS? Choose an answer from the below options.

AWS Directory Service for Microsoft Active Directory (Enterprise Edition)
Any of these options are acceptable to use as long as they configured correctly for 10,000 customers
Simple AD
✅ AD Connector

Explanation:-For the exam, remember the usage of the following AD options: SimpleAD: Microsoft Active Directory compatible directory from AWS Directory Service and supports common features of an active directory. AWS Directory Service for Microsoft Active Directory: Managed Microsoft

Active Directory that is hosted on AWS cloud. AD Connector: Proxy service for connecting your on-premises Microsoft Active Directory to the AWS cloud. Option A is incorrect because SimpleAD does not connect existing on-premises AD to AWS. Option B is incorrect because AWS Directory Service for Microsoft AD is an AWS managed service that is hosted on the AWS cloud, it does not connect your AD with AWS. Option C is CORRECT because AD Connector helps connecting your on-premises Microsoft Active Directory to the AWS cloud. Option D is incorrect because none of the options above are acceptable except AD Connector. The below diagram shows how to use the AD directory connect service for using existing on-premises directory with AWS services. https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html The correct answer is: AD Connector

---

Q11)

You are designing a social media site and are considering how to mitigate distributed denial-of-service (DDoS) attacks.

Which of the below are viable mitigation techniques? Choose 3 options from the below

- Use dedicated instances to ensure that each instance has the maximum performance possible.
- ✅ Use an Amazon CloudFront distribution for both static and dynamic content.

Explanation:-This question is asking you to select some of the most recommended and widely used DDoS mitigation techniques. What is a DDoS Attack? A Distributed Denial of Service (DDoS) attack is an attack orchestrated by distributed multiple sources that makes your web application unresponsive and unavailable for the end users. DDoS Mitigation Techniques Some of the recommended techniques for mitigating the DDoS attacks are (i) build the architecture using the AWS services and offerings that have the capabilities to protect the application from such attacks. e.g. CloudFront, WAF, Autoscaling, Route53, VPC etc. (ii) defend the infrastructure layer by over-provisioning capacity, and deploying DDoS mitigation systems. (iii) defend the application layer by using WAF, and operating at scale by using autoscale so that the application can withstand the attack by scaling and absorbing the traffic. (iv) minimizing the surface area of attack (v) obfuscating the AWS resources Option A is incorrect because ENIs do not help in increasing the network bandwidth. Option B is incorrect because having dedicated instances performing at maximum capacity will not help mitigating the DDoS attack. What is needed is instances behind auto-scaling so that the traffic can be absorbed while actions are being taken on the attack and the application can continue responding to the clients. Option C is CORRECT because (a) CloudFront is AWS managed service and it can scale automatically, (b) helps absorbing the traffic, and (c) it can help putting restriction based on geolocation. i.e. if the attack is coming from IPs from specific location, such requests can be blocked. Option D is CORRECT because (a) ELB helps distributing the traffic to the instances that are part of auto-scaling (helps absorbing the traffic), and (b) Amazon RDS is an Amazon managed service which can withstand the DDoS attack. Option E is CORRECT because CloudWatch can help monitoring the network traffic as well as CPU Utilization for suspicious activities. Option F is incorrect because adding and removing rules of firewall is not going to mitigate the DDoS attack. It is very important to read the AWS Whitepaper on Best Practices for DDoS Resiliency. https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf The correct answers are: Use an Amazon CloudFront distribution for both static and dynamic content., Use an Elastic Load Balancer with auto scaling groups at the web, App. Restricting direct internet traffic to Amazon Relational Database Service (RDS) tiers., Add alert Amazon CloudWatch to look for high network in and CPU utilization.

- ✅ Use an Elastic Load Balancer with auto scaling groups at the web, App. Restricting direct internet traffic to Amazon Relational Database Service (RDS) tiers.

Explanation:-(a) CloudFront is AWS managed service and it can scale automatically, (b) helps absorbing the traffic, and (c) it can help putting restriction based on geolocation. i.e. if the attack is coming from IPs from specific location, such requests can be blocked.

(a) ELB helps distributing the traffic to the instances that are part of auto-scaling (helps absorbing the traffic), and (b) Amazon RDS is an Amazon managed service which can withstand the DDoS attack.

CloudWatch can help monitoring the network traffic as well as CPU Utilization for suspicious activities.

- ✅ Add alert Amazon CloudWatch to look for high network in and CPU utilization.

Explanation:-This question is asking you to select some of the most recommended and widely used DDoS mitigation techniques. What is a DDoS Attack? A Distributed Denial of Service (DDoS) attack is an attack orchestrated by distributed multiple sources that makes your web application unresponsive and unavailable for the end users. DDoS Mitigation Techniques Some of the recommended techniques for mitigating the DDoS attacks are (i) build the architecture using the AWS services and offerings that have the capabilities to protect the application from such attacks. e.g. CloudFront, WAF, Autoscaling, Route53, VPC etc. (ii) defend the infrastructure layer by over-provisioning capacity, and deploying DDoS mitigation systems. (iii) defend the application layer by using WAF, and operating at scale by using autoscale so that the application can withstand the attack by scaling and absorbing the traffic. (iv) minimizing the surface area of attack (v) obfuscating the AWS resources Option A is incorrect because ENIs do not help in increasing the network bandwidth. Option B is incorrect because having dedicated instances performing at maximum capacity will not help mitigating the DDoS attack. What is needed is instances behind auto-scaling so that the traffic can be absorbed while actions are being taken on the attack and the application can continue responding to the clients. Option C is CORRECT because (a) CloudFront is AWS managed service and it can scale automatically, (b) helps absorbing the traffic, and (c) it can help putting restriction based on geolocation. i.e. if the attack is coming from IPs from specific location, such requests can be blocked. Option D is CORRECT because (a) ELB helps distributing the traffic to the instances that are part of auto-scaling (helps absorbing the traffic), and (b) Amazon RDS is an Amazon managed service which can withstand the DDoS attack. Option E is CORRECT because CloudWatch can help monitoring the network traffic as well as CPU Utilization for suspicious activities. Option F is incorrect because adding and removing rules of firewall is not going to mitigate the DDoS attack. It is very important to read the AWS Whitepaper on Best Practices for DDoS Resiliency. https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf The correct answers are: Use an Amazon CloudFront distribution for both static and dynamic content., Use an Elastic Load Balancer with auto scaling groups at the web, App. Restricting direct internet traffic to Amazon Relational Database Service (RDS) tiers., Add alert Amazon CloudWatch to look for high network in and CPU utilization.

Q12) As an AWS administrator, what is the best way to configure the NAT instance with fault tolerance? Choose the correct answer from the below options.

- Create two NAT instances in a public subnet; create a route from the private subnet to each NAT instance for fault tolerance
- Create one NAT instance in a public subnet; create a route from the private subnet to that NAT instance.
- ✅ Create two NAT instances in two separate public subnet; create a route from the private subnet to each NAT instance for fault tolerance

Explanation:-You should place two NAT instances in two separate public subnets, and create route from instances via each NAT instance for achieving fault tolerance. More information on NAT instances: One approach to this situation is to leverage multiple NAT instances that can take over for each other if the other NAT instance should fail. This walkthrough and associated monitoring script (nat_monitor.sh) provide instructions for building a HA scenario where two NAT instances in separate Availability Zones (AZ) continuously monitor each other. If one NAT instance fails, this script enables the working NAT instance to take over outbound traffic and attempts to fix the failed instance by stopping and restarting it. Below is a diagram for fault tolerant NAT instances.

- Create two NAT instances in two separate private subnets.

Q13)

There is a requirement for a company to transfer large amounts of data between AWS and an on-premise location.

There is an additional requirement for low latency and high consistency traffic to AWS.

Out of these given requirements, how would you design a hybrid architecture? Choose the correct answer from the below options.

- ✅ Provision a Direct Connect connection to an AWS region using a Direct Connect partner.
- Create an IPSec tunnel for private connectivity which increases network consistency and reduces latency.
- Create a VPN tunnel for private connectivity which increases network consistency and reduces latency.
- This is not possible.

Explanation:-Tip: Whenever he scenario in the question requires the use of low latency transfer of data between AWS/VPC and on premise servers/database, always think about provisioning AWS Direct Connect. Option A is CORRECT because Direct Connect creates a dedicated connection between AWS and on premises server for low latency secured transfer of data. Option B is incorrect because setting up VPN connectivity has higher cost as well as setup and maintenance overhead compared to Direct Connect. Also, Direct Connect provides a dedicated network connection bypassing the internet. Hence it is more secure. Option C is incorrect because setting up IPSec tunnel has setup and maintenance overhead. Also, IPSec tunnel does not guarantee the end-to-end security of the data as it uses internet. Option D is incorrect as Direct Connect is the most suited option for this scenario. More information on AWS Direct Connect: AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. For more information on AWS direct connect, just browse to the below URL: https://aws.amazon.com/directconnect/ The correct answer is: Provision a Direct Connect connection to an AWS region using a Direct Connect partner.

Q14)

You are developing a new mobile application and are considering storing user preferences in AWS.

This would provide a more uniform cross-device experience to users using multiple mobile devices to access the application.

The preference data for each user is estimated to be 50KB in size. Additionally, 5 million customers are expected to use the application on a regular basis.

The solution needs to be cost-effective, highly available, scalable and secure.

How would you design a solution to meet the above requirements?

- ✅ Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table. Utilize STS. Web Identity Federation, and DynamoDB Fine Grained Access Control to authenticate and authorize access.
- Setup an RDS MySQL instance in 2 availability zones to store the user preference data. Deploy a public facing application on a server in front of the database to manage security and access credentials
- Setup an RDS MySQL instance with multiple read replicas in 2 availability zones to store the user preference data .The mobile application will query the user preferences from the read replicas. Leverage the MySQL user management and access privilege system to manage security and access credentials.
- Store the user preference data in S3. Setup a DynamoDB table with an item for each user and an item attribute pointing to the user' S3 object. The mobile application will retrieve the S3 URL from DynamoDB and then access the S3 object directly utilize STS, Web identity Federation, and S3 ACLs to authenticate and authorize access.

Explanation:-(a) it uses DynamoDB for scalability and cost efficiency, (b) It uses federated acccess using Web Identity Provider, and (c) uses fine grained access priviledges for authenticating the access.

Q15) Which feature of S3 needs to be enabled for a resource in a bucket in one domain to access a resource in a bucket in another domain? Choose an answer from the below options.

- Modify bucket policy to allow cross domain access.
- ✅ You can configure your bucket to explicitly enable cross-origin requests from the other domain.
- Modify the ACL policy to allow cross domain access.

Explanation:-CORS enables a resource in one bucket access a resource in another. More information on CORS: Cross-Origin Resource Sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS support in Amazon S3, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.

- This is not possible

Q16)

You want to migrate an EC2 instance from one region to another and use the same PEM keys.

How will you accomplish this?

- Copy AMI of your EC2 machine between regions and start an instance from that AMI
- Use copy key command line API to transfer key to different regions
- Key pair is not a region level concept, all the keys are available globally

Explanation:-Key pairs across regions is not possible. In order to use key pairs across regions you need to import the key pairs in the respective regions. You need to go the respective region and from the EC2 dashboard , click on Import Key pair and choose the relevant key pair.

- ✅ Using import key-pair feature using AWS web console

Q17)

As an AWS Administrator, there is a requirement to monitor all changes in an AWS environment and all traffic sent to and from the environment.

Which of the following 2 options can you take into consideration to ensure the requirements are met?

✅ Configure an IPS/IDS system, such as Palo Alto Networks, that monitors, filters, and alerts of all potential hazard traffic leaving the VPC.
⚪ Configure an IPS/IDS system, such as Palo Alto Networks, using promiscous mode that monitors, filters, and alerts of all potential hazard traffic leaving the VPC.
⚪ Configure an IPS/IDS in promiscuous mode, which will listen to all packet traffic and API changes.
✅ Configure an IPS/IDS to listen and block all suspected bad traffic coming into and out of the VPC. Configure CloudTrail with CloudWatch Logs to monitor all changes within an environment.
Explanation:-(a) it detects and blocks the malicious traffic coming into and out of VPC, and (b) it also leverages CloudTrail logs and CloudWatch to monitor all the changes in the environment.
it monitors, filters, and alerts about the potentially hazardous traffic leaving from VPC. Please find the below developer forums thread on the same.

Q18)

To serve Web traffic for a popular product your chief financial officer and IT director have purchased 10 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 c4.2xlarge medium utilization RI.

You register the two c4.2xlarge instances with your ELB and quickly find that the large instances are at 100% of capacity and the c4.2xlarge instances have a significant capacity that's unused.

Which option is the most cost-effective and uses EC2 capacity most effectively?

⚪ Configure ELB with two c4.2xlarge Instances and use on-demand Autoscaling group for up to two additional c4.2xlarge instances.
⚪ Route traffic to EC2 large and c4.2xlarge 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 Autoscaling group and Launch Configuration with ELB to add up to 10 more on-demand mi large instances when triggered by Cloudwatch shut off c4.2xiarge instances
Explanation:-In this question, the problem is that the newly added c4.2xlarge instances are not fully utilized. This is happening because the load is spread evenly across all the instances. There is no logic on how much traffic is to be routed to which instance types. Hence, there is need to add some logic where higher (more-weighted) traffic should be routed to c4.2xlarge instances and light-weighted to the other instances. Route 53's weighted routing policy does exactly this, so you should look for this option. Option A is CORRECT because it first creates separate ELBs, one each for set of different instance type and uses Route 53's weighted routing policy such that the load is distributed as per the heaviness of the traffic to appropriate instance type. Option B is incorrect because shutting down c4.2xlarge instances will not be an effective use of the EC2 capacity. You have already paid for the instance. So you would lose money here. Option C is incorrect because latency based routing may not always distribute heavy traffic to the large instance. You must use weighted routing policy. Option D is incorrect because this option is not a good use of the existing capacity, and in fact, would add to the cost. For more information on Route 53 weighted routing policy, please visit the URL below: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-weighted The correct answer is: Use a separate ELB for each instance type and distribute load to ELBs with Route 53 weighted round robin

---

Q19)

A company has 2 VPC's in the same region.

How can you connect the VPC's so that EC2 instances in one VPC can communicate with the other VPC? Choose an answer from the below options.

⚪ Migrate each VPC resources from one VPC using migration tools such as Import/Export, Snapshot, AMI Copy, and S3 sharing.
✅ Create a VPC peering connection between each VPC.
⚪ Create an OpenVPN instance in one VPC and establish an IPSec tunnel between VPCs.
⚪ Create a Direct Connect connection from one VPC endpoint to the other VPC.
Explanation:-VPC peering is the best way of connecting the EC2 instances in two VPCs in the same region.

Q20)

Your company produces customer commissioned one-of-a-kind skiing helmets combining high fashion with custom technical enhancements.

The current manufacturing process is data rich and complex including assessments to ensure that the custom electronics and materials used to assemble the helmets are to the highest standards.

Assessments are a mixture of human and automated assessments you need to add a new set of assessment to model the failure modes of the custom electronics using GPUs across a cluster of servers with low latency networking.

What architecture would allow you to automate the existing process using a hybrid approach and ensure that the architecture can support the evolution of processes over time?

⚪ Use AWS Data Pipeline to manage movement of data & meta-data and assessments. Use an auto-scaling group of G2 instances in a placement group.
✅ Use Amazon Simple Workflow (SWF) to manage assessments, movement of data & meta-data. Use an autoscaling group of G2 instances in a placement group.
⚪ Use Amazon Simple Workflow (SWF) to manage assessments movement of data & meta-data. Use an autoscaling group of C3 instances with SR-IOV (Single Root I/O Virtualization).
⚪ Use AWS data Pipeline to manage movement of data & meta-data and assessments. Use auto-scaling group of C3 with SR-IOV (Single Root I/O virtualization).
Explanation:-(a) it uses G2 instances which are specialized for high graphical processing of data with low latency networking, and (b) SWF supports workflows involving human interactions along with AWS services.

Q21)

You are running a successful multitier web application on AWS and your marketing department has asked you to add a reporting tier to the application.

The reporting tier will aggregate and publish status reports every 30 minutes from user-generated information that is being stored in your web application's database.

You are currently running a Multi-AZ RDS MySQL instance for the database tier.

You also have implemented Elasticache as a database caching layer between the application tier and database tier.

Select the answer that will allow you to successfully implement the reporting tier with as little impact as possible to your database.

- Generate the reports by querying the ElasliCache database caching tier.
- Generate the reports by querying the synchronously replicated standby RDS MySQL instance maintained through Multi-AZ.
- ✅ Launch a RDS Read Replica connected to your Multi AZ master database and generate reports by querying the Read Replica.
- Continually send transaction logs from your master database to an S3 bucket and generate the reports off the S3 bucket using S3 byte range requests.

Explanation:-In question is asking you to design a reporting layer with least impact on the database. If the reporting queries are fired on the database instance, the performance of the database instance would surely get impacted. Since querying for the report would be a read heavy operation, the best solution is to create the read replicas of the database instance and query on them rather than on the database instance. This way, the existing database instance will have the least impact.
It uses the Read Replicas of the database for the querying of reports.

Q22)

Your department creates regular analytics reports from your company's log files.

All log data is collected in Amazon S3 and processed by daily Amazon Elastic MapReduce (EMR) jobs that generate daily PDF reports and aggregated tables in CSV format for an Amazon Redshift data warehouse.

Your CFO requests you to optimize the cost structure for this system.

Which of the following alternatives will lower costs without compromising the average performance of the system or data integrity for the raw data?

- Use Reduced Redundancy Storage (RRS) for all data in Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
- Use Reduced Redundancy Storage (RRS) for PDF and CSV data in Amazon S3. Add Spot instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
- ✅ Use Reduced Redundancy Storage (RRS) for PDF and CSV files in S3. Use a combination of Spot instances and Reserved Instances for Amazon EMR jobs. Use Reserved instances for Amazon Redshift.
- Use Reduced Redundancy Storage (RRS) for all data in S3. Use a combination of Spot instances and Reserved Instances for Amazon EMR jobs. Use Spot Instances for Amazon Redshift.

Explanation:-There are 3 main considerations in this question - Cost optimization, Average Performance should not be compromised, and Data integrity should be preserved. Since the log files are getting stored on S3, the Reduced Redundancy Storage (RRS) provides the reduce storage cost (Cost Optimization) as well as preserves the data integrity. Note that the RRS has reduced durability (99.99% compared to 99.999999999% of S3), but does not compromise with data integrity. To maintain the average performance of data processing, instances must be reserved so that there would bu guaranteed availability of the compute resources. Additionally, you can use spot instances which are more cost effective compared to reserved instances to increase the overall performance of processing of the log files. Option A is incorrect because if only spot instances are used for data processing, the average performance could be hampered as the availability of spot instance is not always guaranteed (The availability of spot instances depend on the available capacity and spot price. AWS can terminate the spot instances if the spot price exceeds your maximum price). Option B is CORRECT because (a) You need to store only the PDF and CSV files in RRS, not the entire data as these files can be generated by the EMR jobs in case of loss of data, and (b) The combination of the reserved and spot will guarantee the average performance and it will help reduce cost (by not reserving all the instances, only reserving the required instances). Moreover, AWS RRS would reduce cost and guarantee data integrity as discussed above. Option C is incorrect because (a) You should not store the entire data on RRS as this storage class is only for the data that is noncritical, and reproducible, and (b) If only spot instances are used for data processing, the average performance could be hampered as the availability of spot instance is not always guaranteed (The availability of spot instances depend on the available capacity and spot price. AWS can terminate the spot instances if the spot price exceeds your maximum price). Option D is incorrect because you should not store the entire data on RRS as this storage class is only for the data that is noncritical, and reproducible. If the data is lost, the PDF and CSV files cannot be regenerated.
The correct answer is: Use Reduced Redundancy Storage (RRS) for PDF and CSV files in S3. Use a combination of Spot instances and Reserved Instances for Amazon EMR jobs. Use Reserved instances for Amazon Redshift.

Q23)

You are designing a data leak prevention solution for your VPC environment. You want your VPC Instances to be able to access software depots and distributions on the Internet for product updates.

The depots and distributions are accessible via the third party via their URLs.

You want to explicitly deny any other outbound connections from your VPC instances to hosts on the internet.

Which of the following options would you consider?

- Implement security groups and configure outbound rules to only permit traffic to software depots.
- ✅ Configure a web proxy server in your VPC and enforce URL-based rules for outbound access. Remove default routes.
- Implement network access control lists to allow traffic from specific destinations, with an implicit deny as a rule.
- Move all your instances into private VPC subnets. Remove default routes from all routing tables and add specific routes to the software depots and distributions only.

Explanation:-There are 3 main considerations in this scenario: (a) the instances in your VPC needs internet access, (b) the access should be restricted for product updates only, and (c) all other outbound connection requests must be denied. With such scenarios, you should not put your instances in public subnet as they would have access to internet without any restrictions. So, you should put them in a private subnet, and since there is a need of a logic for filtering the requests from client machines, configure a proxy server. What is a Proxy Server? Proxy server is a server

that acts as a mediator between client(s) that sends requests and server that receives the requests and replies back. If any client requires any resources, it connects to the proxy server, and the proxy server evaluates the request based on its filtering rules. If the requests are valid, it connects to the server which receives the request and replies back. The proxy server also maintains cache; i.e., if any subsequent requests from same or other clients are received, it returns the result from the cache, saving the trip to and from the server. Hence, proxy servers tend to improve the performance. See the diagram below: Option A is CORRECT because a proxy server (a) filters requests from the client, and allows only those that are related to the product updates, and (b) in this case helps filtering all other requests except the ones for the product updates. Option B is incorrect because a security group cannot filter request based on URLs and you cannot specify deny rules. Option C is incorrect because even though moving the instances in a private subnet is a good idea, the routing table does not have the filtering logic, it only connects the subnets with internet gateway. Option D is incorrect because you are trying to deny the outbound traffic from your VPC. There is no need for any traffic to be allowed in. An example of setting up a proxy server can be found via the below URL: https://aws.amazon.com/articles/6463473546098546 The correct answer is: Configure a web proxy server in your VPC and enforce URL-based rules for outbound access. Remove default routes.

Q24)

A company is building a voting system for a popular TV show, viewers watch the performances then visit the show's website to vote for their favorite performer.

It is expected that in a short period of time after the show is finished the site will receive millions of visitors.

The visitors will the first login to the site using their Amazon.com credentials and then submit their vote.

After the voting is completed the page will display the vote totals.

The company needs to build the site such that can handle the rapid influx of traffic while maintaining good performance but also wants to keep costs to a minimum.

Which of the design patterns below should they use?

- Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first login with Amazon service to authenticate the user, the web servers will process the users vote and store the result into a DynamoDB table using IAM Roles for EC2 instances to gain permissions to the DynamoDB table.
- ✅ Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first login with Amazon service to authenticate the user, the web servers will process the users vote and store the result into an SQS queue using IAM Roles for EC2 Instances to gain permissions to the SQS queue. A set of application servers will then retrieve the items from the queue and store the result into a DynamoDB table.
- Use CloudFront and an Elastic Load balancer in front of an auto-scaled set of web servers, the web servers will first login with the Amazon service to authenticate the users, then process the users vote and store the result into a multi-AZ Relational Database Service instance.
- Use CloudFront and the static website hosting feature of S3 with the Javascript SDK to call the login with Amazon service to authenticate the user, use IAM Roles to gain permissions to a DynamoDB table to store the users vote.

Explanation:-This scenario has following architectural considerations:(1) the application need to be scalable so that it can handle traffic coming from millions of users, (2) the application should handle rapid influx of traffic maintaining good performance, and (3) the cost should be kept to minimum. When the application needs to handle the data coming from millions of users, always think about using DynamoDB. Also, to provide the global users with high performance content access, you need to consider CloudFront, and you need to set the appropriate IAM Role for the front end / web servers to give access to DynamoDB tables. Option A is incorrect because multi-AZ RDS is expensive solution compared to DynamoDB. Option B is incorrect because although this would work, it is not scalable and storing all the data directly in DynamoDB would consume read and write capacity and increase the cost. Option C is incorrect because it is not scalable and storing all the data directly in DynamoDB would consume read and write capacity and increase the cost. Option D is CORRECT because (a) it is highly scalable, (b) creates appropriate IAM Role to access the DynamoDB database, and (c) more importantly uses SQS to hold the user data/votes such that the application does not consume read and write provisioned capacity of DynamoDB. The correct answer is: Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first login with Amazon service to authenticate the user, the web servers will process the users vote and store the result into an SQS queue using IAM Roles for EC2 Instances to gain permissions to the SQS queue. A set of application servers will then retrieve the items from the queue and store the result into a DynamoDB table.

Q25)

A company is trying to migrate all of their applications to the cloud.

But they have a legacy based application that is built on TCP.

The application is built to work on ports 80 and 8080.

There is a requirement to have ELB and Auto Scaling to ensure traffic is routed properly and scalability of the application.

What listener configuration would you create on the ELB? Choose an answer from the below option.

- ✅ Configure the load balancer with the following ports: TCP:80 and TCP:8080 and the instance protocol to TCP:80 and TCP:8080
- Configure the load balancer with the following ports: HTTP:80 and HTTP:8080 and the instance protocol to HTTP:80 and HTTP:8080
- Configure the load balancer with the following ports: HTTP:80 and HTTP:8080 and the instance protocol to HTTPs:80 and HTTPs:8080
- Configure the load balancer with the following ports: HTTP:80 and HTTP:8080 and the instance protocol to TCP:80 and TCP:8080

Explanation:-The application in this scenario is a legacy based application that is built on TCP and works on ports 80 and 8080. It requires that the traffic should be routed correctly. Option A is CORRECT, because for the ELB to route the traffic correctly, it should be configured with ports TCP:80 and TCP 8080. For the backends as well, the ports that should be configured must be TCP:80 an TCP:8080. Option B, C, and D are all incorrect as both the ELB and instance protocol must be configured for ports TCP:80 and TCP:8080. More information on ELB Since the application is a custom application and not a standard HTTP application, hence you need to have the TCP ports open. Hence option A is the right option. Before you start using Elastic Load Balancing, you must configure one or more listeners for your Classic Load Balancer. A listener is a process that checks for connection requests. It is configured with a protocol and a port for front-end (client to load balancer) connections, and a protocol and a port for back-end (load balancer to back-end instance) connections. Elastic Load Balancing supports the following protocols: HTTP HTTPS (secure HTTP) TCP SSL (secure TCP) For more information on listener configuration for ELB please see the below link http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html The correct answer is: Configure the load balancer with the following ports: TCP:80 and TCP:8080 and the instance protocol to TCP:80 and TCP:8080

Q26)

A read-only news reporting site with a combined web and application tier and a database tier that receives large and unpredictable traffic demands must be able to respond to these traffic fluctuations automatically.

What should AWS services be used meet these requirements?

✅ Stateless instances for the web and application tier synchronized using Elasticache Memcached in an autoscaling group monitored with CloudWatch and RDS with read replicas for the backend.
⚪ Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch and RDS with read replicas.
⚪ Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch and multi-AZ RDS
⚪ Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch and multi-AZ RDS
Explanation:-The scenario asks for 2 things: (1) a performance improving solution for read heavy web tier and database tier. Hint: Always see if any of the options contain caching solution such as ElastiCache, CloudFront, or Read Replicas, and (2) whether to use stateless or stateful instances. Stateful instances are not suitable for distributed systems, as they the state or connection between client and web server, database remains engaged as long as the session is active. Hence, it increases the load on the server as well as database. Stateless instances, however are distributed and easy to scale in/scale out. Hence, the stateless application tend to improve the performance of a distributed application. Option A is CORRECT because (a) it uses stateless instances, (b) the web server uses ElastiCache for read operations, (c) it uses CloudWatch which monitors the fluctuations in the traffic and notifies to auto-scaling group to scale in/scale out accordingly, and (d) it uses read replicas for RDS to handle the read heavy workload. Option B is incorrect because (a) it uses stateful instances, and (b) it does not use any caching mechanism for web and application tier. Option C is incorrect because (a) it uses stateful instances, (b) it does not use any caching mechanism for web and application tier, and (c) multi-AZ RDS does not improve read performance. Option D is incorrect because multi-AZ RDS does not improve read performance. For more information on ElastiCache and Read Replicas, please refer to the following links: https://aws.amazon.com/elasticache/ https://aws.amazon.com/rds/details/read-replicas/ The correct answer is: Stateless instances for the web and application tier synchronized using Elasticache Memcached in an autoscaling group monitored with CloudWatch and RDS with read replicas for the backend.

Q27)

There is a requirement to have the read replica of a running MySQL RDS instance inside of AWS to an on-premise location.

What is the securest way of performing this replication? Choose the correct answer from the below options.

⚪ RDS cannot replicate to an on-premise database server. Instead, first configure the RDS instance to replicate to an EC2 instance with core MySQL, and then configure replication over a secure VPN/VPG connection.
✅ Create an IPSec VPN connection using either OpenVPN or VPN/VGW through the Virtual Private Cloud service.
⚪ Configure the RDS instance as the master and enable replication over the open internet using a secure SSL endpoint to the on-premise server.
⚪ Create a Data Pipeline that exports the MySQL data each night and securely downloads the data from an S3 HTTPS endpoint.
Explanation:-It is feasible to setup the secure IPSec VPN connection between the on premise server and AWS VPC using the VPN/Gateways.

Q28)

A company has recently started using Docker cloud. This is a SaaS solution for managing Docker containers on the cloud.

There is a requirement for the SaaS solution to access AWS resources.

Which of the following options would meet the requirement for enabling the SaaS solution to work with AWS resources in the most secured manner?

⚪ From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.
✅ Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
⚪ Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application. Create a new access and secret key for the user and provide these credentials to the SaaS provider.
⚪ Create an IAM role for EC2 instances, assign it a policy that allows only the actions required tor the Saas application to work, provide the role ARM to the SaaS provider to use when launching their application instances.
Explanation:-When a user, a resource, an application, or any service needs to access any AWS service or resource, always prefer creating appropriate role that has least privileged access or only required access, rather than using any other credentials such as keys. Option A is incorrect because you should never share your access and secret keys. Option B is incorrect because (a) when a user is created, even though it may have the appropriate policy attached to it, its security credentials are stored in the EC2 which can be compromised, and (b) creation of the appropriate role is always the better solution rather than creating a user. Option C is CORRECT because AWS role creation allows cross-account access to the application to access the necessary resources. See the image and explanation below: Many SaaS platforms can access AWS resources via a Cross-account access created in AWS. If you go to Roles in your identity management, you will see the ability to add a cross-account role. Option D is incorrect because the role is to be assigned to the application and it's resources, not the EC2 instances. For more information on the cross-account role, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html The correct answer is: Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.

Q29)

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 organization want access to that same restored data via their EC2 instances in your VPC.

What of the following would be the optimal setup for persistence and security that meets the above requirements?

⚪ 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.
⚪ 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 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.

Explanation:-The main consideration in this question is: only the EC2 instances in your VPC you should be able to access RDS instances and the setup should support persistence. Option A is incorrect because RDS instance will be part of the Elastic Beanstalk environment and would not be optimal for performance. Option B is incorrect because you should always use the DNS endpoint of the RDS instance, not IP address as this option suggests. Option C is CORRECT because (a) it uses RDS instance separately (not part of Beanstalk), (b) it uses DNS name of RDS for accessing it, and (c) it correctly configures the security group such that only the valid client machines have access to RDS instance. Option D is incorrect because the security group is not configured correctly as it gives access to all the hosts in the application subnets. The correct answer is: 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.

Q30)

You have an application running on an EC2 Instance which will allow users to download files from a private S3 bucket using a pre-signed URL.

Before generating the URL, the application should verify the existence of the file in S3.

How should the application use AWS credentials to access the S3 bucket securely?

Create an IAM user for the application with permissions that allow list access to the S3 bucket. The application retrieves the IAM user credentials from a temporary directory with permissions that allow read access only to the application user.

Create an IAM role for EC2 that allows list access to objects in the S3 bucket. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata

Use the AWS account access Keys. The application retrieves the credentials from the source code of the application.

Create an IAM user for the application with permissions that allow list access to the S3 bucket launch the instance as the IAM user and retrieve the IAM user's credentials from the EC2 instance user data.

Explanation:-An IAM role is similar to a user. In that, it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user. You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. Whenever the question presents you with a scenario where an application, user, or service wants to access another service, always prefer creating IAM Role over IAM User. The reason being that when an IAM User is created for the application, it has to use the security credentials such as access key and secret key to use the AWS resource/service. This has security concerns. Whereas, when an IAM Role is created, it has all the necessary policies attached to it. So, the use of access key and secret key is not needed. This is the preferred approach. Option A is incorrect because you should not use the account access keys , instead you should use the IAM Role. Option B is incorrect because instead of IAM User, you should use the IAM Role. See the explanation given above. Option C is CORRECT because, (a) it creates the IAM Role with appropriate permissions, and (b) the application accesses the AWS Resource using that role. Option D is incorrect because instead of IAM User, you should use the IAM Role. See the explanation given above. For more information on IAM roles, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html The correct answer is: Create an IAM role for EC2 that allows list access to objects in the S3 bucket. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata

---

Q31)

A newspaper organization has an on-premises application which allows the public to search its back catalog and retrieve individual newspaper pages via a website written in Java.

They have scanned the old newspapers into JPEGs which is of a total size of 17TB and used Optical Character Recognition (OCR) to populate a commercial search product.

The hosting platform and software now end of life and the organization wants to migrate its archive to AWS and produce a cost-efficient architecture and still be designed for availability and durability.

Which of the below options is the most appropriate?

Use a CloudFront download distribution to serve the JPEGs to the end users and Install the current commercial search product, along with a Java Container for the website on EC2 instances and use Route53 with DNS round-robin.

Model the environment using CloudFormation. Use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the JPEGs and search index.

Use S3 with reduced redundancy to store and serve the scanned files. Use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones.

Use a single-AZ RDS MySQL instance to store the search index for the JPEG images and use an EC2 instance to serve the website and translate user queries into SQL.

Explanation:-This question presents following scenarios: (1) type of storage that can store large amount of data (17TB), (2) the commercial search product is at its end of life, (3) the architecture should be cost effective, highly available, and durable. Tip: Whenever a storage service that can store large amount of data with low cost, high availability, and high durability, always think about using S3. Option A is incorrect because even though it uses S3, it uses the commercial search software which is at its end of life. Option B is incorrect because striped EBS is not as durable solution as S3 and certainly not as cost effective as S3. Also, it has maintenance overhead. Option C is CORRECT because (a) it uses S3 RRS to store the images which is cost-effective, (b) instead of the commercial product that is at its end of life, it uses CloudSearch for query processing, and (c) with multi AZ implementation, it achieves high availability. Option D is incorrect because with single AZ RDS instance, it does not have high availability. Option E is incorrect because (a) this configuration is not scalable, and (b) it does not mention any origin for the CloudFront distribution. Amazon CloudSearch With Amazon CloudSearch, you can quickly add rich search capabilities to your website or application. You don't need to become a search expert or worry about hardware provisioning, setup, and maintenance. With a few clicks in the AWS Management Console, you can create a search domain and upload the data that you want to make searchable, and Amazon CloudSearch will automatically provision the required resources and deploy a highly tuned search index. You can easily change your search parameters, fine tune search relevance, and apply new settings at any time. As your volume of data and traffic fluctuates, Amazon CloudSearch seamlessly scales to meet your needs. For more information on AWS CloudSearch, please visit the below link https://aws.amazon.com/cloudsearch/ The correct answer is: Use S3 with reduced redundancy to store and serve the scanned files. Use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones.

Q32)

You're running an application on-premises due to its dependency on non-x86 hardware and want to use AWS for data backup.

Your backup application is only able to write to POSIX-compatible block-based storage.

You have 624TB of data and would like to mount it as a single folder on your file server.

Users must be able to access portions of this data while the backups are taking place.

What backup solution would be most appropriate for this use case?

- Configure your backup software to use Glacier as the target for your data backups.
- ✅ Use Storage Gateway and configure it to use Gateway Cached volumes.
- Configure your backup software to use S3 as the target for your data backups.

Explanation:-Gateway-Cached volumes can support volumes of 1,024TB in size, where as Gateway-stored volume supports volumes of 512 TB size. Option A is CORRECT because (a) it supports volumes of upto 1,024TB in size, and (b) the frequently accessed data is store on the on-premise server while the entire data is backed up over AWS. Option B is incorrect because S3 is not ideal for POSIX compliant data. Option C is incorrect because the data stored in Amazon Glacier is not available immediately. Retrieval jobs typically require 3–5 hours to complete; so, if you need immediate access to your data as mentioned in the question, this may not be the ideal choice. Option D is incorrect because gateway stored volumes can only store only 512TB worth of data. For more information on all of the options for storage please refer to the below link http://docs.aws.amazon.com/storagegateway/latest/userguide/resource-gateway-limits.html#resource-volume-limits

- Use Storage Gateway and configure it to use Gateway Stored volumes.

Q33)

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

Your servers 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 from the below:

- Data encryption across the Internet
- Data integrity protection across the Internet
- Peer identity authentication between VPN gateway and customer gateway

Explanation:-The data that is transiting via the IPSec tunnel is encrypted.
IPSec protects the data that is in transit over the internet (fundamental responsibility of IPSec tunnel). Option E is CORRECT because in this scenario, the IPSec tunnel is established between VPN gateway (VPG) and Customer Gateway (CGW) whose identity gets authenticated during the setup of the IPSec tunnel.
As mentioned earlier - integrity of the data that is transiting via the IPSec tunnel is always preserved (fundamental responsibility of IPSec tunnel).

- Protection of data in transit over the Internet
- ✅ All of these

Q34)

You have instances in a public subnet which downloads patches from the internet in addition to serving clients on the normal HTTP protocol.

There is a requirement to ensure that just the serving protocol and the URL's listed to get the patches are accessible from the instances.

Which of the following options would you consider?

- ✅ Configure a web proxy server in your VPC and enforce URL-based rules for outbound access. Remove default routes.
- Implement security groups and configure outbound rules to only permit traffic to the url's.
- Move all your instances into private VPC subnets. Remove default routes from all routing tables and add specific routes to the software depots and distributions only.
- Implement network access control lists to all specific destinations, with an Implicit deny as a rule.

Explanation:-There are 3 main considerations in this scenario: (a) the instances in your VPC needs internet access, (b) the access should be restricted for product updates only, and (c) all other outbound connection requests must be denied. With such scenarios, you should not put your instances in public subnet as they would have access to internet without any restrictions. So, you should put them in a private subnet, and since there is a need of a logic for filtering the requests from client machines, configure a proxy server. What is a Proxy Server? Proxy server is a server that acts as a mediator between client(s) that sends requests and server that receives the requests and replies back. If any client requires any resources, it connects to the proxy server, and the proxy server evaluates the request based on its filtering rules. If the requests are valid, it connects to the server which receives the request and replies back. The proxy server also maintains cache; i.e., if any subsequent requests from same or other clients are received, it returns the result from the cache, saving the trip to and from the server. Hence, proxy servers tend to improve the performance. See the diagram below: Option A is CORRECT because a proxy server (a) filters requests from the client, and allows only those that are related to the product updates, and (b) in this case helps filtering all other requests except the ones for the product updates. Option B is incorrect because a security group cannot filter request based on URLs. Option C is incorrect because even though moving the instances in a private subnet is a good idea, the routing table does not have the filtering logic, it only connects the subnets with internet gateway. Option D is incorrect because a security group cannot filter request based on URLs. An example of setting up a proxy server can be found via the below URL: https://aws.amazon.com/articles/6463473546098546 The correct answer is: Configure a web proxy server in your VPC and enforce URL-based rules for outbound access. Remove default routes.

Q35)

A company is running a batch analysis every hour on their main transactional DB running on an RDS MySQL instance to populate their central Data Warehouse running on Redshift.

During the execution of the batch their transactional applications are very slow.

When the batch completes they need to update the top management dashboard with the new data.

The dashboard is produced by another system running on-premises that is currently started when a manually-sent email notifies that an update is required.

The on-premises system cannot be modified because is managed by another team.

How would you optimize this scenario to solve performance issues and automate the process as much as possible?

- Replace RDS with Redshift for the oaten analysis and SQS to send a message to the on-premises system to update the dashboard
- ✅ Create an RDS Read Replica for the batch analysis and SNS to notify me on-premises system to update the dashboard
- Create an RDS Read Replica for the batch analysis and SQS to send a message to the on-premises system to update the dashboard.
- Replace RDS with Redshift for the batch analysis and SNS to notify the on-premises system to update the dashboard

Explanation:-There are two architectural considerations here. (1) you need to improve read performance by reducing the load on the RDS MySQL instance, and (2) automate the process of notifying to the on-premise system. When the scenario asks you to improve the read performance of a DB instance, always look for options such as ElastiCache or Read Replicas. And when the question asks you to automate the notification process, always think of using SNS. Option A is incorrect because Redshift is used for OLAP scenarios whereas RDS is used for OLTP scenarios. Hence, replacing RDS with Redshift is not a solution. Option B is incorrect because Redshift is used for OLAP scenarios whereas RDS is used for OLTP scenarios. Hence, replacing RDS with Redshift is not a solution. Option C is CORRECT because (a) it uses Read Replicas which improves the read performance, and (b) it uses SNS which automates the process of notifying the on-premise system to update the dashboard. Option D is incorrect because SQS is not a service to be used for sending the notification.

Q36)

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 decision is made to use multi-AZ RDS MySQL instance 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 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 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 Cross-Zone support in the application Use an ELB 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 ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two application servers in different AZs.

Explanation:-AWS ELB has support for Proxy Protocol. It simply depends on a humanly readable header with the client's connection information to the TCP data sent to your server. As per the AWS documentation, the Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connections. Because load balancers intercept traffic between clients and your instances, the access logs from your instance contain the IP address of the load balancer instead of the originating client. You can parse the first line of the request to retrieve your client's IP address and the port number. Option A is CORRECT because it implements the proxy protocol and uses ELB with TCP listener. Option B is incorrect because, although implementing cross-zone load balancing provides high availability, it is not going to give the IP address of the clients. Option C is incorrect because Route53 latency based routing does not give the IP address of the clients. Option D is incorrect because Route53 Alias record does not give the IP address of the clients. For more information on ELB enabling support for TCP, please refer to the links given below: https://aws.amazon.com/blogs/aws/elastic-load-balancing-adds-support-for-proxy-protocol/ https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-proxy-protocol.html The correct answer is: File a change request to implement Proxy Protocol Support. In the application use an ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two application servers in different AZs.

Q37)

Your company is planning to develop an application in which the front end is in .Net and the backend is in DynamoDB.

There is expectant of a high load on the application.

How could you ensure the scalability and cost-effectiveness of the application to reduce the load on the DynamoDB database? Choose an answer from the below options.

- ✅ Use SQS to hold the database requests instead of overloading the DynamoDB database. Then have a service that asynchronously pull the messages and write them to DynamoDB.
- Add more DynamoDB databases to handle the load.
- Increase write capacity of Dynamo DB to meet the peak loads.

Explanation:-This question is asking for an option that can be used to reduce the load on DynamoDB database. The option has to be scalable. In such scenario, the best option to use is SQS, because it is scalable and cost efficient as well. Option A is incorrect because adding more databases is not going to reduce the load on existing DynamoDB databses. Also, this is not a cost efficient solution. Option B is incorrect because increasing the write capacity is an expensive option. Option C is CORRECT because it uses SQS to assist in taking over the load from storing the data in DynamoDB, and it is scalable as well as cost efficient. Option D is incorrect because MultiAZ configuration is not going to help reduce the load, in fact it will affect the performance as the records in DynamoDB would get replicated in multiple availability zones. More information on SQS: When the idea comes for scalability then SQS is the best option. Normally DynamoDB is scalable, but since one is looking for a cost effective solution, the messaging in SQS can assist in managing the situation mentioned in the question. Amazon Simple Queue Service (SQS) is a fully-managed message queuing service for reliably communicating among distributed software components and microservices - at any scale. Building applications from individual components that each perform a discrete function improves scalability and reliability, and is best practice design for modern applications. SQS makes it simple and cost-effective to decouple and coordinate the components of a cloud application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available For more information on SQS, please refer to the below url https://aws.amazon.com/sqs/ The correct answer is: Use SQS to hold the database requests instead of overloading the DynamoDB database. Then have a service that asynchronously pull the messages and write them to

DynamoDB.
- Launch DynamoDB in Multi-AZ configuration with a global index to balance writes.

Q38)

Your company has recently extended its data center into a VPC on AWS to add burst computing capacity as needed.

Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary.

You don't want to create new IAM users for each member and make those users sign in again to the AWS Management Console.

Which option below will meet the needs of your NOC members?

- Use OAuth 2.0 to retrieve temporary AWS security credentials to enable your members to sign in to the AWS Management Console.
- Use your on-premises SAML 2.0-compliant identity provider (IDP) to retrieve temporary security credentials to enable members to sign in to the AWS Management Console.
- ✅ Use your on-premises SAML 2.0-compliant identity provider (IDP) to grant the members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint
- Use web Identity Federation to retrieve AWS temporary security credentials to enable your members to sign in to the AWS Management Console.

Explanation:-(a) it gives a federated access to the NOC members to AWS resources by using SAML 2.0 identity provider, and (b) it uses on-premise single sign on (SSO) endpoint to authenticate users and gives them access tokens prior to providing the federated access.

Q39)

Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high-resolution MP4 format.

Your workforce is distributed globally often on the move and using company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video.

Your company has no video transcoding expertise and it required you may need to pay for a consultant.

How would you implement the most cost-efficient architecture without compromising high availability and quality of video delivery'?

- A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days CloudFront to serve HLS transcoded videos from EC2.
- ✅ Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. Use S3 to host videos with Lifecycle Management to archive original flies to Glacier after a few days. Use CloudFront to serve HLS transcoded videos from S3.
- Elastic Transcoder to transcode original high-resolution MP4 videos to HLS EBS volumes to host videos and EBS snapshots to incrementally backup original rues after a few days. CloudFront to serve HLS transcoded videos from EC2.
- A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number or nodes depending on the length of the queue. Use S3 to host videos with Lifecycle Management to archive all files to Glacier after a few days. Use CloudFront to serve HLS transcoding videos from Glacier.

Explanation:-(a) it uses Amazon Elastic Transcoder that converts from MP4 to HLS, (b) S3 Object Lifecycle Management reduces the cost by archiving the files to Glacier, and (c) CloudFront - which is a highly available service - enables the global delivery of the video without compromising the video delivery speed or quality.

Q40) As an AWS Cloud Architect professional , In Cloudfront what is the Origin Protocol policy that must be chosen to ensure that the communication with the origin is done either via http or https. Choose an answer from the options below

- ✅ Match Viewer

Explanation:-If the Origin Protocol Policy is set to Match Viewer, the CloundFront communicates with the origin using HTTP or HTTPS depending on the protocol of the viewer request. For more information on Cloudfront CDN please see the below link: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html The correct answer is: Match Viewer

- None of these
- HTTP
- HTTPS

Q41)

As an AWS Cloud Architect professional you have been instructed to share files via S3.

But since these files are confidential, they cannot be accessed directly and need to be accessed via Cloudfront.

Which of the below additional configurations need to be carried out to complete this requirement?

- 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 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.
- Create individual policies for each bucket the documents are stored in and in that policy grant access to CloudFront only.

Explanation:-It gives CloudFront the exclusive access to S3 bucket, and prevents other users from accessing the public content of S3 directly via S3 URL.

Q42)

You are looking to migrate your Development and Test environments to AWS.

You have decided to use separate AWS accounts to host each environment.

You plan to link each accounts bill to a Master AWS account using Consolidated Billing.

To make sure you keep within the budget, you would like to implement a way for administrators in the Master account to have access to stop, delete and/or terminate resources in both the Dev and Test accounts.

Identify which of the options will allow you to achieve this goal.

✅ Create IAM users in the Master account. Create cross-account roles in the Dev and Test accounts that have full Admin permissions and grant the Master account access.
⚪ Create IAM users and a cross-account role in the Master account that grants full Admin permissions to the Dev and Test accounts.
⚪ Link the accounts using Consolidated Billing. This will give IAM users in the Master account access to resources in the Dev and Test accounts
⚪ Create IAM users in the Master account with full Admin permissions. Create cross-account roles in the Dev and Test accounts that grant the Master account access to the resources in the account by inheriting permissions from the Master account.
Explanation:-the cross-account role is created in Dev and Test accounts, and the users are created in the Master account, that are given that role.

Q43)

You currently operate a web application in the AWS US-East region. The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database.

Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2, IAM and RDS resources.

The solution must ensure the integrity and confidentiality of your log data.

Which of the below solutions would you recommend?

⚪ Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected. Use S3 ACLs and Multi Factor Authentication (MFA) to delete on the S3 bucket that stores your logs
✅ Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles S3 bucket policies and Multi Factor Authentication (MFA) to delete on the S3 bucket that stores your logs.
⚪ Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs.
⚪ Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.
Explanation:-(a) it uses AWS CloudTrail with Global Option enabled, (b) a single new S3 bucket and IAM Roles so that it has the confidentiality, (c) MFA on Delete on S3 bucket so that it maintains the data integrity. See the AWS CloudTrail setting below which sets the Global Option.

Q44)

Your company has 2 departments that want to use Redshift.

One department uses a process that takes 3 hours to analyze the data whereas the second department just takes a few minutes.

What can you do to ensure that there is no performance impact and delete to the second's department's queries? Choose an answer from the below options.

⚪ Pause long queries and resume the queries afterwards
⚪ Create a read replica of the Red shift instance and run second department's queries on read replica
✅ Create two separate workload management groups and assign them to respective departments
⚪ Start another Redshift cluster from snapshot for the second department if current Redshift cluster is busy processing long queries
Explanation:-The best solution - without any effect on performance - is to create two separate workload management groups - one for each department and run the queries on them. See the image below: More information on Amazon Redshift Workload Management Amazon Redshift Workload Management (WLM) enables users to flexibly manage priorities within workloads so that short, fast-running queries won't get stuck in queues behind long-running queries. Amazon Redshift WLM creates query queues at runtime according to service classes, which define the configuration parameters for various types of queues, including internal system queues and user-accessible queues. From a user perspective, a user-accessible service class and a queue are functionally equivalent. For consistency, this documentation uses the term queue to mean a user-accessible service class as well as a runtime queue.

Q45) What are the benefits of using an IPSec tunnel from connecting from an on-premise location to AWS? Choose 4 correct options from the below:

✅ Data encryption across the Internet
⚪ End-to-end Identity authentication
✅ Peer identity authentication between VPN gateway and customer gateway
✅ Data integrity protection across the Internet
Explanation:-IPSec is designed to provide authentication, integrity, and confidentiality of the data that is being transmitted. IPSec operates at network layer of the OSI model. Hence, it only protects the data that is in transit over the internet. For the full security of the data transmission it is very essential that both the sender and receiver need to be IPSec-aware. Option A is incorrect because (a) IPSec operates at network layer of the OSI model. Hence, it only protects the data that is in transit over the internet, and (b) both the source and the destination (client and server) may not be IPSec aware. IPSec protects the data that is in transit over the internet (fundamental responsibility of IPSec tunnel). Option E is CORRECT because in this scenario, the IPSec tunnel is established between VPN gateway (VPG) and Customer Gateway (CGW) whose identity gets authenticated during the setup of the IPSec tunnel. Integrity of the data that is transiting via the IPSec tunnel is always preserved (fundamental responsibility of IPSec tunnel).
⚪ End-to-end protection of data in transit
✅ Protection of data in transit over the Internet

Q46)

Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your AWS resources.

The solution must ensure the integrity and confidentiality of your log data.

Which of these solutions would you recommend?

○ Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.
○ Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected. Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
✓ Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
○ Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs.
Explanation:-(a) it uses AWS CloudTrail with Global Option enabled, (b) a single new S3 bucket and IAM Roles so that it has the confidentiality, (c) MFA on Delete on S3 bucket so that it maintains the data integrity. See the AWS CloudTrail setting below which sets the Global Option.

Q47)

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 all 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 form the options below

✓ You are running the proxy on a small-sized EC2 instance in a private subnet and its network throughput is being throttled by a NAT running on an undersized EC2 instance
✓ 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.
○ You are running the proxy in a public subnet but have not allocated enough EIP's to 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 fail.
Explanation:-This scenario contains following main points: (1) there is a single EC2 instance running proxy software that either itself acts as or connects to a NAT instance. The NAT instances are not AWS managed, they are user managed; so, it may become the bottleneck, (2) there is a whitelist maintained so that the outside access to the instances inside VPC has limited access, (3) the URLs in the whitelist are correctly maintained, so whitelist is not an issue, (4) only some machines are having download problems with some updates. i.e. some updates are successful on some machines. This indicates that there is no setup issue, but most-likely it is the proxy instance that is a bottleneck and under-performing or inconsistently performing. As the proxy instance is not part of any auto-scaling group, it's size must be definitely the issue. Option A is CORRECT because due to limited size of proxy instance, it's network throughput might not be sufficient to provide service to all the VPC instances (as only some of the instances are not able to download the updates). Option B is incorrect because limited storage on the proxy instance should not cause other instances any problems in downloading the updates. Option C is incorrect because proxy instances are supposed to be in public subnet, but allocation of EIPs should not cause any issues for other instances in the VPC. Option D is CORRECT because undersized NAT instance can be a bottleneck and can cause other instances suffer from insufficient network throughput. Option E is incorrect because if this was the case, none of the instances would get the updates. However, some of the instances were able to get the updates, so, this cannot be the case. The correct answers are: 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., You are running the proxy on a small-sized EC2 instance in a private subnet and its network throughput is being throttled by a NAT running on an undersized EC2 instance

---

Q48)

You are designing a multi-platform web application for AWS. The application will run on EC2 instances and will be accessed from PCs, tablets, and smartphones.

Supported accessing platforms are Windows.

MACOS, IOS, and Android. Separate sticky session and SSL certificate setups are required for different platform types.

Which of the following describes the most cost-effective and performance efficient architecture setup?

○ Set up one ELB for all platforms to distribute load among multiple instance under it. Each EC2 instance implements ail functionality for a particular platform.
○ Set up two ELBs. The first ELB handles SSL certificates for all platforms and the second ELB handles session stickiness for all platforms for each ELB run separate EC2 instance groups to handle the web application for each platform.
✓ Assign multiple ELBS to an EC2 instance or group of EC2 instances running the common components of the web application, one ELB for each platform type Session stickiness and SSL termination are done at the ELBs
○ Setup a hybrid architecture to handle session state and SSL certificates on-premise and separate EC2 Instance groups running web applications for different platform types running in a VPC.
Explanation:-In this scenario, the main architectural considerations are (1) web application has EC2 instances running multiple platforms such as Android, iOS etc., and (2) separate sticky session and SSL certificate setups are required for different platforms. The best approach is to create 3 separate ELBs, per platform type. Option A is incorrect because it is not cost effective to handle such hybrid architecture. Option B is incorrect because if you create a single ELB for all these EC2 instances, distributing the load based on the platform type and managing the different sticky session and SSL certificate requirements will be very cumbersome and may not be feasible at all. Option C is incorrect because ELB cannot handle multiple SSL certificates. Option D is CORRECT because (a) it creates separate ELBs for each platform type, so the distribution of the load based on platform type becomes much more convenient and effective, and (b) each ELB can handle its own sticky session and SSL termination logic.

Q49)

Your company is hosting an application on the cloud. Your IT Security department has recently noticed that there seem to be some SQL Injection attacks against the application.

Which of the below approach provides a cost-effective scalable mitigation to this kind of attack?

- Add previously identified host file source IPs as an explicit INBOUND DENY NACL to the web tier subnet.
- Remove all but TLS 1 & 2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.
- ✅ Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group
- Create a DirectConnect connection so that your have a dedicated connection line.

Explanation:-(a) WAF Tiers acts as the first line of defense, it filters out the known sources of attack and blocks common attack patterns, such as SQL injection or cross-site scripting, (b) the ELB of the application is not exposed to the attack, and most importantly (c) this pattern - known as "WAF Sandwich" pattern - has WAF layer with EC2 instances are placed between two ELBs - one that faces the web, receives all the traffic, and sends them to WAF layer to filter out the malicious requests, and sends the filtered non-malicious requests, another ELB - which receives the non-malicious requests and send them to the EC2 instances for processing.

Q50)

A company has a legacy based software which needs to be transferred to the AWS cloud. The legacy based software has a dependency on the license which is based on the MAC Address.

What would be a possible solution to ensure that the legacy based software will work properly always and not lose the MAC address at any point in time? Choose an answer from the below options.

- Make sure any EC2 Instance that you deploy has a static IP address that is mapped to the MAC address.
- Use a VPC with a private subnet and configure the MAC address to be tied to that subnet.
- Use a VPC with a private subnet for the license and a public subnet for the EC2.

Explanation:-You should use Elastic Network Interface that is associated with a fixed MAC address. This will ensure that the legacy license based software would always work and not lose the MAC address any point in future.

- ✅ Use a VPC with an elastic network interface that has a fixed MAC Address.
