Answer Sheet

Q1)

A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC.

The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24.

What will happen in this scenario?

● It is not possible to create a subnet with the same CIDR as the VPC

● The second subnet will be created

✓ It will throw a CIDR overlap error

Explanation:-Since the CIDR of the new subnet overlaps with that of the first subnet, an overlap error will be displayed. See the snapshot below: For more information on VPC subnets, please refer to the below link http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html The correct answer is: It will throw a CIDR overlap error

● The VPC will modify the first subnet to allow this IP range

---

Q2)

Your company has just set up a new central server in a VPC.

There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server.

Which of the below options is best suited to achieve this requirement?

● Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.

✓ Set up VPC Peering between the central server VPC and each of the teams VPCs.

Explanation:-VPC Peering allows multiple VPCs to route traffic between them using the private IP addresses of the EC2 instances. Option B is incorrect because you cannot setup DirectConnect between different VPCs. Option C is incorrect because you cannot setup IPSec tunnel between different VPCs. Option D is incorrect as the correct solution is to use VPC Peering. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region.

● Set up AWS DirectConnect between the central server VPC and each of the teams VPCs.

● None of these options will work.

Q3)

You've been hired to enhance the overall security posture for a very large e-commerce site. They have a well architected multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3.

They are using a combination of RDS and DynamoDB for their dynamic data and then archiving nightly into S3 for further processing with EMR.

They are concerned because they found questionable log entries and suspect someone is attempting to gain unauthorized access.

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

● Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to their VPC. Then they would establish Internet connectivity into their space, filter the traffic in hardware Web Application Firewall (WAF) and then pass the traffic through the DirectConnect connection into their application running in their VPC.

● 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

Explanation:-In such scenarios where you are designing a solution to prevent the DDoS attack, always think of using Web Access Firewall (WAF). AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns. Option A is incorrect because, although this option could work, the setup is very complex and it is not a cost effective solution. Option B is incorrect because, (a) even though blocking certain IPs will mitigate the risk, the attacker could maneuver the IP address and circumvent the IP check by NACL, and (b) it does not prevent the attack from the new source of threat. Option C is CORRECT because (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. See the image below: Option D is incorrect because there is no such thing as Advanced Protocol Filtering feature for ELB. For more information on WAF, please visit the below URL: https://aws.amazon.com/waf/ The correct answer is: 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

---

Q4) As an IT administrator, you have created a VPC with CIDR block 10.0.0.0/24. As per your knowledge, as an AWS Cloud professional, what is the maximum allowed numbers of IP addresses and the minimum allowed numbers of IP addresses

according to AWS and what is the number of IP addresses supported by the VPC you created? Choose the correct answer from the below options.

● Maximum is 256 and the minimum is 16 and the one created supports 24 IP addresses
● Maximum is 28 and the minimum is 16 and the one created supports 24 IP addresses
● Maximum is 65,536 and the minimum is 24 and the one created supports 28 IP addresses
✓ Maximum is 65,536 and the minimum is 16 and the one created supports 256 IP addresses
Explanation:-First let us calculate the current number of IP addresses. The CIDR block is 10.0.0.0/24. Hence, out of 32 bits of address, 24 bits are set/masked. Hence, the remaining 8 bits indicate the remaining available IP addresses. Hence, the total number of current available instances is 2^(32-24) = 2^8 = 256. Now, the maximum allowed block size is a /16 netmask. i.e. Out of 32, first 16 bits are set/masked, leaving 16 bits available. Hence, the total number of maximum available instances = 2^(32-16) = 2^16 = 65,536. Now, the minimum allowed block size is a /28 netmask. i.e Out of 32, first 28 bits are set/masked, leaving 4 bits available. Hence, the total number of minimum available instances = 2^(32-28) = 2^4 = 16.

Q5)

There is a requirement for a web-based application hosted on AWS to talk to Redshift tables.

Which of the below options best suited to have this in place from a security standpoint?

● Create an IAM user and generate encryption keys for that user. Create a policy for RedShift read-only access. Embed the keys in the application.
● Create a HSM client certificate in Redshift and authenticate using this certificate.
● Create a RedShift read-only access policy in IAM and embed those credentials in the application.
✓ Use roles that allow a web identity federated user to assume a role that allows access to the RedShift table by providing temporary credentials.
Explanation:-(a) IAM role allows the least privileged access to the AWS resource, (b) web identity federation ensures the identity of the user, and (c) the user is given temporary credentials to access the AWS resource.

Q6)

An AWS customer is deploying an application that is composed of an AutoScaling group of EC2 Instances. The customer's security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique x 509 certificate that contains the specific instance ID.

In addition, an x 509 certificates must be designed by the customer's Key management service in order to be trusted for authentication.

Which of the following configurations will support these requirements?

● Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group Have the launched instances, generate a certificate signature request with the instance's assigned instance-id to the Key management service for signature.
● Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure me Auto Scaling group to launch instances with this role. Have the instances bootstrap, get the certificate from Amazon S3 upon first boot.
✓ Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the Key management, service generate a signed certificate and send it directly to the newly launched instance.
Explanation:-(a) once the instance is launched in the auto scaling group, it notifies the key management service to generate a signed certificate, (b) the key management service is trusted, and (c) once the certificate is generated, it is directly sent to the newly created instance; hence, the workflow is logical.
● Configure the launched instances to generate a new certificate upon first boot. Have the Key management, service poll the AutoScaling group for associated instances and send new instances a certificate signature (that contains the specific instance-id.

Q7)

You require the ability to analyze a customer's clickstream data on a website so they can do the behavioral analysis.

Your customer needs to know what sequence of pages and ads their customer clicked on.

This data will be used in real time to modify the page layouts as customers click through the site to increase stickiness and advertising click-through.

Which option meets the requirements for captioning and analyzing this data?

● Write click events directly to Amazon Redshift and then analyze with SQL
● Publish web clicks by session to an Amazon SQS queue and periodically drain these events to Amazon RDS and analyze with sql.
● Log clicks in weblogs by URL and store it in Amazon S3, and then analyze with Elastic MapReduce
✓ Push web clicks by session to Amazon Kinesis and analyze behavior using Kinesis workers
Explanation:-Whenever the question presents a scenario where the application needs to do analysis on real time data such as clickstream (i.e.massive real-time data analysis), most of the time the best option is Amazon Kinesis. It is used to collect and process large streams of data records in real time. You'll create data-processing applications, known as Amazon Kinesis Streams applications. A typical Amazon Kinesis Streams application reads data from an Amazon Kinesis stream as data records. These applications can use the Amazon Kinesis Client Library, and they can run on Amazon EC2 instances. The processed records can be sent to dashboards, used to generate alerts, dynamically change pricing and advertising strategies, or send data to a variety of other AWS services

Q8) What should you consider when you try to implement an IDS infrastructure on AWS? Choose 2 correct options from the below:

✓ Implement a reverse proxy layer in front of web servers and configure IDS/IPS agents on each reverse proxy server.
Explanation:-The main responsibility of Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) is to (a) detect the vulnerabilities in your EC2 instances, (b) protect your EC2 instances from attacks, and (c) respond to intrusion or attacks against your EC2 instances. The IDS is an appliance that is installed on the EC2 instances that continuously monitors the VPC environment to see if any malicious activity is happening and alerts the system administration if such activity is detected. IPS, on the other hand, is an appliance that is installed on the EC2 instances that monitors and analyzes the incoming and outgoing network traffic for any malicious activities and prevents the malicious requests from reaching to the instances in the VPC. This scenario is asking you how you can setup IDS/IPS in your VPC. There are few well known ways: (a) install the IDS/IPS

agents on the EC2 instances of the VPC, so that the activities of that instance can be monitored, (b) set up IDS/IPS on a proxy server/NAT through whichthe network traffic is flowing, or (c) setup a Security-VPC that contains EC2 instances with IDS/IPS capability and peer that VPC with your VPC and always accept the traffic from Security-VPC only. It implements the IDS/IPS agents on each EC2 instances in the VPC. ELB with SSL is does not have the intrusion detection/prevention capability.

● Configure an instance in each subnet to switch its network interface card to promiscuous mode and analyze network traffic.
✓ Implement IDS/IPS agents on each Instance running In VPC
Explanation:-The main responsibility of Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) is to (a) detect the vulnerabilities in your EC2 instances, (b) protect your EC2 instances from attacks, and (c) respond to intrusion or attacks against your EC2 instances. The IDS is an appliance that is installed on the EC2 instances that continuously monitors the VPC environment to see if any malicious activity is happening and alerts the system administration if such activity is detected. IPS, on the other hand, is an appliance that is installed on the EC2 instances that monitors and analyzes the incoming and outgoing network traffic for any malicious activities and prevents the malicious requests from reaching to the instances in the VPC. This scenario is asking you how you can setup IDS/IPS in your VPC. There are few well known ways: (a) install the IDS/IPS agents on the EC2 instances of the VPC, so that the activities of that instance can be monitored, (b) set up IDS/IPS on a proxy server/NAT through whichthe network traffic is flowing, or (c) setup a Security-VPC that contains EC2 instances with IDS/IPS capability and peer that VPC with your VPC and always accept the traffic from Security-VPC only. It implements the IDS/IPS agents on each EC2 instances in the VPC. ELB with SSL is does not have the intrusion detection/prevention capability.
● Implement Elastic Load Balancing with SSL listeners In front of the web applications

Q9) An internal auditor has been assigned to view your company's internal AWS services. As an AWS administrator, what is the best solution to provide the auditor so that he can carry out the required auditing services? Choose the correct answer from the below options.

● Create an IAM user with full VPC access but set a condition that will not allow him to modify anything if the request is from any IP other than his own.
● Give the auditor root access to your AWS Infrastructure.
● Create an IAM user tied to an administrator role. Also, provide an additional level of security with MFA
✓ Create an IAM Role with the read only permissions to access the AWS VPC infrastructure and assign that role to the auditor.
Explanation:-Generally, you should refrain from giving high-level permissions and give only the required permissions. In this case, it fits well by just providing the relevant access which is required. IAM Role gives just the minimum required permissions (read-only) to audit the VPC infrastructure to the auditor.

Q10)

An auditor has been assigned to view all the logs of your AWS environment.

Which of the below options would be the best solution for the auditor to ensure that they can view the logs in the AWS environment?

● Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
✓ Enable CloudTrail logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.
Explanation:-You need to enable the CloudTrail logging in order to generate the logs with information about all the activities related to the AWS account and resources. It also creates an IAM user that has permissions to read the logs that are stored in the S3 bucket. More information on AWS CloudTrail AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.
● The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.
● Create a role that has the required permissions for the auditor.

Q11)

A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS which includes a NAT (Network Address Translation) instance in the public Web tier.

There is enough provisioned capacity for the expected workload for the new fiscal year benefit enrollment period plus some extra overhead.

Enrollment proceeds nicely for two days and then the web tier becomes unresponsive, upon investigation using CloudWatch and other monitoring tools.

It is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a country where the benefits company has no customers.

The web tier instances are so overloaded that benefit enrolment administrators cannot even SSH into them.

Which activity would be useful in defending against this attack?

● Create 15 Security Group rules to block the attacking IP addresses over port 80
● Change the EIP (Elastic IP Address) of the NAT instance in the web tier subnet and update the Main Route Table with the new EIP
● Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (internet Gateway)
✓ Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses
Explanation:-(a) you can add deny rules in NACL and block access to certain IP addresses.

Q12)

Your company has recently extended its datacenter into a VPC on AWS.

There is a requirement for on-premise users manages AWS resources from the AWS console.

You don't want to create IAM users for them again.

Which of the below options will fit your needs for authentication?

✓ Use your on-premises SAML 2 O-compliant identity provider (IDP) to grant the members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.
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.
● Use web Identity Federation to retrieve AWS temporary security credentials to enable your members to sign in to the AWS Management Console.
● 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 SAML2.0-compliant identity provider (IDP) to retrieve temporary security credentials to enable members to sign in to the AWS Management Console.

Q13)

There is a requirement for an application hosted on AWS to work with DynamoDB tables.

Which of the following is the best option for the application hosted on an EC2 instance to work with the data in the DynamoDB table? Choose the correct answer from the below options.

● Create an IAM user and assign the IAM user to a group with proper permissions to communicate with DynamoDB
● Create an IAM group that only gives access to your application and to the DynamoDB tables. Then, when writing to DynamoDB, simply include the unique device ID to associate the data with that specific user.
✓ Create an IAM role with the proper permission policy to communicate with the DynamoDB table. Use web identity federation, which assumes the IAM role using AssumeRoleWithWebIdentity. when the user signs in, granting temporary security credentials using STS.
Explanation:-(a) creates an IAM Role with the needed permissions to connect to DynamoDB, (b) it authenticates the users with Web Identity Federation, and (c) the application accesses the DynamoDB with temporary credentials that are given by STS.
● Create an Active Directory server and an AD user for each mobile application user. When the user signs in to the AD sign-on, allow the AD server to federate using SAML 2.0 to IAM and assign a role to the AD user which is the assumed with AssumeRoleWithSAML.

Q14)

Your firm has uploaded a large amount of aerial image data to S3. In the past, in your on-premises environment, you used a dedicated group of servers to process this data and used Rabbit MQ

– An open source messaging system to get job information to the servers.

Once processed the data would go to the tape and be shipped offsite.

Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost.

Which of the following options is correct?

● Change the storage class of the S3 objects to Reduced Redundancy Storage. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS. Once data is processed, change the storage class of the S3 objects to Glacier.
● Use SNS to pass job messages use Cloud Watch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.
✓ Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS. Once data is processed, change the storage class of the S3 objects to Glacier
Explanation:-The most suggestive hint in this question is that it asks you to leverage AWS archival storage and messaging services. Hence, you should look for options Glacier and SQS. Option A is incorrect because (a) RRS is not an archival storage option, and (b) since auto scaling is not mentioned, you cannot use CloudWatch alarms to terminate the idle EC2 instances. Option B is CORRECT because (a) it uses SQS to process the messages, (b) it uses Glacier as the archival storage solution - which is cost optimized. Option C is incorrect because RRS is not an archival storage option. Option D is incorrect as SNS cannot be use to process the messages. i.e. it cannot replace the functionality that was getting provided by RabbitMQ. The correct answer is: Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS. Once data is processed, change the storage class of the S3 objects to Glacier
● Use SQS for passing job messages. Use Cloud Watch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.

Q15)

There is a requirement to change the DHCP options set with a VPC.

Which of the following options do you need to take to achieve this?

● You can modify the options from the console or the CLI.
● You need to stop all the instances in the VPC. You can then change the options, and they will take effect when you start the instances.
● You can modify the options from the CLI only, not from the console.
✓ You must create a new set of DHCP options and associate them with your VPC
Explanation:-As per the AWS documentation, once you create a set of DHCP options, you cannot modify them. For more information on DHCP Options set please see the below link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html The correct answer is: You must create a new set of DHCP options and associate them with your VPC.

Q16)

A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC) and is connected to the corporate data center via an IPsec VPN.

The application must authenticate against the on-premises LDAP server.

After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user.

Which two approaches can satisfy these objectives? Choose 2 options from the below

✓ Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service (STS) to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.
Explanation:-There are two architectural considerations here: (1) The users must be authenticated via the on-premise LDAP server, and (2) each user should have access to S3 only. With this information, it is important to first authenticate the users using LDAP, get the IAM Role name, then get the temporary credentials from STS, and finally access the S3 bucket using those credentials. And second, create an IAM Role that provides access to S3. Option A is incorrect because the users need to be authenticated using LDAP first, not STS. Also, the temporary credentials to log into AWS are provided by STS, not identity broker. Option B is CORRECT because it follows the correct sequence. It authenticates users using LDAP, gets the security token from STS, and then accesses the S3 bucket using the temporary credentials. Option C is CORRECT because it follows the correct sequence. It develops an identity broker that authenticates users against LDAP, gets the security token from STS, and then accesses the S3 bucket using the IAM federated user credentials. Option D is incorrect because you cannot use the LDAP credentials to log into IAM. For more information on federated access, please visit the below link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html The correct answers are: The application authenticates against LDAP and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service (STS) to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket., Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service (STS) to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.

● Develop an identity broker that authenticates against IAM Security Token Service (STS) to assume a IAM role in order to get temporary AWS security credentials The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.

● The application authenticates against LDAP the application then calls the AWS identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials the application can use the IAM temporary credentials to access the appropriate S3 bucket.

✓ The application authenticates against LDAP and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service (STS) to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket.

Explanation:-There are two architectural considerations here: (1) The users must be authenticated via the on-premise LDAP server, and (2) each user should have access to S3 only. With this information, it is important to first authenticate the users using LDAP, get the IAM Role name, then get the temporary credentials from STS, and finally access the S3 bucket using those credentials. And second, create an IAM Role that provides access to S3. Option A is incorrect because the users need to be authenticated using LDAP first, not STS. Also, the temporary credentials to log into AWS are provided by STS, not identity broker. Option B is CORRECT because it follows the correct sequence. It authenticates users using LDAP, gets the security token from STS, and then accesses the S3 bucket using the temporary credentials. Option C is CORRECT because it follows the correct sequence. It develops an identity broker that authenticates users against LDAP, gets the security token from STS, and then accesses the S3 bucket using the IAM federated user credentials. Option D is incorrect because you cannot use the LDAP credentials to log into IAM. For more information on federated access, please visit the below link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html The correct answers are: The application authenticates against LDAP and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service (STS) to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket., Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service (STS) to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.

Q17)

An administrator in your company has created a VPC with an IPv4 CIDR block 10.0.0.0/24.

Now they want to expand the VPC CIDR because there is a requirement to host more resources in that VPC.

Which of the below requirement can be used to accomplish this? Choose an answer from the below options.

● Create a new VPC with a greater range and then connect the older VPC to the newer one.

● You cannot change a VPC's size. Currently, to change the size of a VPC you must terminate your existing VPC and create a new one.

✓ Expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC
Explanation:-Remember for the exam: In AWS, the CIDR of a VPC can be modified after its creation. Option A is incorrect because you can change the CIDR of VPC by adding upto 4 secondary IPv4 IP CIDRs to your VPC. Option B is CORRECT because you can expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC. Option C is incorrect because deleting the subnets is unnecessary. Option D is incorrect because this configuration would peer the VPC, it will not alter the existing VPC's CIDR. For VPC FAQs, please refer to the following link: https://aws.amazon.com/vpc/faqs/ The correct answer is: Expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC

● Delete all the subnets in the VPC and expand the VPC.

Q18)

An AWS customer runs a public blogging website. The site users upload two million blog entries a month. The average blog entry size is 200 KB.

The access rate to blog entries drops to negligible 6 months after publication and users rarely access a blog entry 1 year after publication.

Additionally, blog entries have a high update rate during the first 3 months following publication, this drops to no updates after 6 months. The customer wants to use CloudFront to improve his user's load times.

Which of the following recommendations would you make to the customer?

● Create a CloudFront distribution with Restrict Viewer Access Forward Query string set to true and minimum TTL of 0.

● Duplicate entries into two different buckets and create two separate CloudFront distributions where S3 access is restricted only to Cloud Front identity

✓ Create a CloudFront distribution with S3 access restricted only to the CloudFront identity and partition the blog entry's location in S3 according to the month it was uploaded to be used with CloudFront behaviors.
Explanation:-The scenario here is that (a) blogs have high access/updates rate in the first 3 months of their creation, (b) this rate drops after 6 months. The main architectural consideration is that the user's load time of the blog needs to be improved. This question is based on making the best use of CloudFront's Cache Behavior. You need to understand two things about CloudFront for such scenario: (1) CloudFront is a service that is designed to give geographically distributed users the fast access to the content by maintaining the content in the cache that is maintained at multiple edge locations, and (2) using the cache-behavior of CloudFront, you can control the origin and path of the content, time to live (TTL), and control the user access using trusted signers. In this scenario, you need to control the content based on the time time period at which the blog is published. i.e. when a blog is published, you need to cache the update for first 3 months, so that it can be quickly accessed by the users, and after six months from the update, the content can be removed from the cache, as it is rarely accessed. Also, you need to make sure that the content is only accessed why

the CloudFront. Option A is incorrect because maintaining two separate buckets is not going to improve the load time for the users. Option B is incorrect as the location-wise distribution is not going to improve the load time for the users. Option C is CORRECT because it (a) the content is only accessed why CloudFront, and (b) if the content is partitioned at the origin based on the month it was uploaded, you can control the cache behavior accordingly, and keep only the latest updated content in the CloudFront cache, so that it can be accessed with fast load-time; hence, improving the performance. Option D is incorrect because, setting minimum TTL of 0 will enforce loading of the content from origin every time, even if it has not been updated over 6 months. For more information on Cloudfront identity, please visit the below link http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html The correct answer is: Create a CloudFront distribution with S3 access restricted only to the CloudFront identity and partition the blog entry's location in S3 according to the month it was uploaded to be used with CloudFront behaviors.

● Create a CloudFront distribution with "US'Europe price class for US/Europe users and a different CloudFront distribution with All Edge Locations' for the remaining users.

Q19)

An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account.

The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party.

Which of the following options would meet all of these conditions?

● Create an IAM role for EC2 instances, assign it a policy which allows only the actions required for the Saas application to work, provide the role ARM to the SaaS provider, to be used when launching their application instances.

● 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.

● 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 that 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.

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 that 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.

Q20)

As an AWS Administrator you are given the following requirement: a. MP4 files needing to be streamed publicly on the company's new video website. b.

The streaming needs to be done on-demand c.

The video files are archived and are expected to be streamed globally, primarily on mobile devices.

Given the above requirements which of the below options will fulfill the above requirements.

● Provision streaming EC2 instances which use S3 as the source for the HLS on-demand transcoding on the servers. Provision a new CloudFront streaming distribution with the streaming server as the origin.

● Upload the MP4 files to S3 and create an Elastic Transcoder job that transcodes the MP4 source into HLS chunks. Store the HLS output in S3 and Configure the Amazon CloudFront distribution with a streaming option to stream the video contents.

● Provision streaming EC2 instances which use S3 as the source for the HLS on-demand transcoding on the servers. Provision a new CloudFront download distribution with the WOWZA streaming server as the origin.

✓ Upload the MP4 files to S3 and create an Elastic Transcoder job that transcodes the MP4 source into HLS chunks. Store the HLS output in S3 and Configure the Amazon CloudFront distribution with a download option to stream the video contents

Explanation:-Tip: In exam, if the question presents a scenario, where the media is to be streamed globally in MP4 format, on multiple platform devices, always think about using Elastic Transcoder. Option A is incorrect because (a) provisioning streaming EC2 instances is a costly solution, (b) the videos are to be delivered on-demand, not live streaming. Option B is incorrect because the videos are to be delivered on-demand, not live streaming. So, streaming server is not required. Option C is CORRECT because it (a) it uses Elastic Transcoder for transcoding the videos to different formats, (b) it uses CloudFront distribution with download option for streaming the on demand videos using HLS on any mobile, and (c) it uses S3 as origin, so keeps the cost low. Option D is incorrect because it uses CloudFront distribution with streaming option; where as, it should use download option. More information on Elastic Transcoder: Amazon Elastic Transcoder manages all aspects of the media transcoding process for you transparently and automatically. There's no need to administer software, scale hardware, tune performance, or otherwise manage transcoding infrastructure. You simply create a transcoding "job" specifying the location of your source media file and how you want it transcoded. Amazon Elastic Transcoder also provides transcoding presets for popular output formats, which means that you don't need to guess about which settings work best on particular devices. For more information on Elastic transcoder please see the below link https://aws.amazon.com/elastictranscoder/ The correct answer is: Upload the MP4 files to S3 and create an Elastic Transcoder job that transcodes the MP4 source into HLS chunks. Store the HLS output in S3 and Configure the Amazon CloudFront distribution with a download option to stream the video contents

---

Q21)

You are designing an SSL/TLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication.

The solution must be resilient.

Which of the following options would you consider for configuring the web server infrastructure? Choose 2 option from the

below

● Configure ELB with HTTPS listeners, and place the Web servers behind it.
● Configure your web servers as the origins for a CloudFront distribution. Use custom SSL certificates on your CloudFront distribution.
✓ Configure ELB with TCP listeners on TCP/443 and place the Web servers behind it.
Explanation:-A reverse proxy server through which the traffic from instances inside VPC flows outside of it, has the IDS/IPS agent installed.
✓ Configure your Web servers with EIP's. Place the Web servers in a Route53 Record Set and configure health checks against all Web servers.
Explanation:-This scenario requires you to setup the web servers in such a way that the HTTPS clients must be authenticated by the client-side certificate (not the server side certificate). There are two ways of architecting this - with ELB and without ELB. (a) With ELB, if you use HTTPS listener, you have to deploy the server side certificate - which is not desired. So, you need to use the TCP listener so that the HTTPS client requests do not terminate at the ELB, they just pass through ELB and terminate at the web server instances. (b) Alternatively, without ELB, you can directly use the web server to communicate with the clients, or set up a Route53 Record Set with the public IP address of the web server(s) such that the client requests would be directly routed to the web server(s). Option A is CORRECT because it uses the TCP (443) listener so that the HTTPS client requests do not terminate at the ELB, they just pass through the ELB and terminate at the web server instances. Option B is CORRECT because it uses Route53 Record Set with the public IP address of the web server(s) such that the client requests would be directly routed to the web server(s). Option C is incorrect because if you use HTTPS listener, you must deploy an SSL/TLS certificate on your load balancer, i.e. authentication via the client certificate is not currently supported. Option D is incorrect because this setting is currently not supported. The correct answers are: Configure ELB with TCP listeners on TCP/443 and place the Web servers behind it., Configure your Web servers with EIP's. Place the Web servers in a Route53 Record Set and configure health checks against all Web servers.

Q22) As a solution architect professional you have been requested to ensure that monitoring can be carried out for EC2 instances which are located in different AWS regions? Which of the below options can be used to accomplish this.

● Create separate dashboards in every region
● Register instances running on different regions to CloudWatch
✓ Have one single dashboard to report metrics to CloudWatch from different region
Explanation:-You can monitor AWS resources in multiple regions using a single CloudWatch dashboard. For example, you can create a dashboard that shows CPU utilization for an EC2 instance located in the US-west-2 region with your billing metrics, which are located in the us-east-1 region. Please see the snapshot below which shows how a global dashboard looks like: Option A is incorrect because you can monitor AWS resources in multiple regions using a single CloudWatch dashboard. Option B is incorrect because you do not need to explicitly register any instances from different regions. Option C is CORRECT because you can monitor AWS resources in multiple regions using a single CloudWatch dashboard. Option D is incorrect because as mentioned in option C, the monitoring of EC2 instances is possible using a single dashboard created from CloudWatch matrix. For more information on Cloudwatch dashboard, please refer to the below URL: http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cross_region_dashboard.html The correct answer is: Have one single dashboard to report metrics to CloudWatch from different region
● This is not possible

Q23)

As an AWS Administrator, you have set up an ELB within a couple of Availability Zones. You have set up a web application on this setup.

You notice that the traffic is not being evenly distributed across the AZ's.

What can be done to alleviate this issue? Choose an answer from the below options.

● Recreate the ELB again.
● Reduce the frequency of the health checks
● Increase the amount of instances hosting the web application in each AZ.
Explanation:-The traffic is not evenly distributed across the instances in multiple AZs. That means the traffic is going to only specific EC2 instances. This happens when either the instances which are not receiving the traffic are unhealthy, or the instances that are receiving the traffic are holding onto the session. This scenario does not mention about any unhealthy instances. So, it is most likely related to instances This situation occurs when ELB has sticky sessions or session affinity enabled.
✓ Disable sticky sessions on the ELB.

Q24)

Your company has an on-premises multi-tier PHP web application, which recently experienced downtime due to a large burst In web traffic due to a company announcement.

Over the coming days, you are expecting similar announcements to drive similar unpredictable bursts, and are looking to find ways to quickly improve your infrastructures ability to handle unexpected increases in traffic.

The application currently consists of a 2 tier web tier which consists of a load balancer and several Linux Apache web servers as well as a database tier which hosts a Linux server hosting a MySQL database.

Which of the below scenario will provide full site functionality, while helping to improve the ability of your application in the short timeframe required?

✓ Offload traffic from on-premises environment by setting up a CloudFront distribution and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behaviour, and select a TTL that objects should exist in cache.
● Create an S3 bucket and configure it tor website hosting. Migrate your DNS to Route53 using zone import and leverage Route53 DNS failover to failover to the S3 hosted website.
● Migrate to AWS. Use VM import 'Export to quickly convert an on-premises web server to an AMI create an Auto Scaling group, which uses the imported AMI to scale the web tier based on incoming traffic. Create an RDS read replica and setup replication between the RDS instance and on-premises MySQL server to migrate the database.
● Create an AMI which can be used of launch web servers in EC2. Create an Auto Scaling group which uses the AMI's to scale the web tier based on incoming traffic. Leverage Elastic Load Balancing to balance traffic between on-premises web servers and those hosted in AWS.
Explanation:-In this scenario, the major points of consideration are: (1) your application may get unpredictable bursts of traffic, (b) you need to improve the current infrastructure in shortest period possible, and (3) your web servers are on premise. Since the time period in hand is short, instead of migrating the app to AWS, you need to consider different ways where the performance would improve without doing much modification to

the existing infrastructure. Option A is CORRECT because (a) CloudFront is AWS's highly scalable, highly available content delivery service, where it can perform excellently even in case of sudden unpredictable burst of traffic, (b) the only change you need to make is make the on-premises load balancer as the custom origin of the CloudFront distribution. Option B is incorrect because you are supposed to improve the current situation in shortest time possible. Migrating to AWS would be more time consuming than simply setting up the CloudFront distribution. Option C is incorrect because you cannot host dynamic web sites on S3 bucket. Also, this option provides insufficient infrastructure set up options. Option D is incorrect because ELB cannot do balancing between AWS EC2 instances and on-premise instances. More information on CloudFront: You can have CloudFront sit in front of your on-premise web environment, via a custom origin. This would protect against unexpected bursts in traffic by letting CloudFront handle the traffic from the cache, thus removing some of the load from the on-premise web servers. Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. Like other AWS services, Amazon CloudFront is a self-service, pay-per-use offering, requiring no long-term. commitments or minimum fees. With CloudFront, your files are delivered to end-users using a global network of edge locations. If you have dynamic content, then it is best to have the TTL set to 0.

Q25)

As an AWS professional, you have been told to ensure that traffic to an application is evenly balanced.

The application has multiple web servers that host the application. Choose an answer from the below options which will fulfill the above requirement.

● Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 ALIAS record to your CloudFront distribution.
● Configure ELB with an EIP. Place all your Web servers behind ELB Configure a Route53 A record that points to the EIP.
✓ Place all your web servers behind ELB. Configure a Route53 ALIAS to point to the ELB DNS name.
● Configure a NAT instance in your VPC Create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address.
Explanation:-(a) if the web servers are behind an ELB, the load on the web servers will be uniformly distributed. Hence, if any of the web servers goes offline or becomes non-responsive, the traffic would be routed to other online web servers; making the application highly available, and (b) You can use Route53 to set the ALIAS record that points to the ELB endpoint.

Q26)

You're building a mobile application game. The application needs permissions for each user to communicate and store data in DynamoDB tables.

What is the best method for granting each mobile device that installs your application to access DynamoDB tables for storage when required? Choose the correct answer from the options below

● Create an Active Directory server and an AD user for each mobile application user. When the user signs in to the AD sign-on, allow the AD server to federate using SAML 2.0 to IAM and assign a role to the AD user which is the assumed with AssumeRoleWithSAML.
● Create an IAM group that only gives access to your application and to the DynamoDB tables. Then, when writing to DynamoDB, simply include the unique device ID to associate the data with that specific user.
● During the install and game configuration process, each user create an IAM credential and assign the IAM user to a group with proper permissions to communicate with DynamoDB.
✓ Create an IAM role with the proper permission policy to communicate with the DynamoDB table. Use web identity federation, which assumes the IAM role using AssumeRoleWithWebIdentity, when the user signs in, granting temporary security credentials using STS.
Explanation:-(a) creates an IAM Role with the needed permissions to connect to DynamoDB, (b) it authenticates the users with Web Identity Federation, and (c) the application accesses the DynamoDB with temporary credentials that are given by STS.

Q27)

You have multiple EC2 instances in three availability zones (AZs), with a load balancer configured for your application.

You observe that only one of those AZs is receiving all the traffic.

How can you ensure that all the AZs receive balanced traffic? Choose two correct answers from the options below:

✓ Enable cross zone load balancer
Explanation:-Cross zone load balancing needs to be enabled on the ELB and the other AZs must be registered under this ELB.
✓ Disable sticky sessions
Explanation:-Cross zone load balancing needs to be enabled on the ELB and the other AZs must be registered under this ELB.
● Reduce the frequency of the health checks
● Amazon recommends to use two availability zone behind ELB

Q28)

You have just developed a new mobile application that handles analytics workloads on large-scale datasets that are stored on Amazon Redshift. Consequently, the application needs to access Amazon Redshift tables.

Which of the following methods would be the best, both practically and security-wise, to access the tables? Choose the correct answer from the options below

● Create a HSM client certificate in Redshift and authenticate using this certificate.
● Create a RedShift read-only access policy in IAM and embed those credentials in the application.
✓ Use roles that allow a web identity federated user to assume a role that allows access to the RedShift table by providing temporary credentials.
Explanation:-(a) IAM role allows the least privileged access to the AWS resource, (b) web identity federation ensures the identity of the user, and (c) the user is given temporary credentials to access the AWS resource.
● Create an IAM user and generate encryption keys for that user. Create a policy for RedShift read-only access. Embed the keys in the application.

Q29)

Your final task that will complete a cloud migration for a customer is to set up an Active Directory service for him so that he can use Microsoft Active Directory with the newly-deployed AWS services.

After reading the AWS documentation for this, you discover that three options are available to set up the AWS Directory Service.

You call the customer to collect more information about his requirements, and he tells you he has 1,000 users on his AD service and wants to be able to use his existing on-premises directory with AWS services.

Which of the following options would be the most appropriate to set up the AWS Directory Service for your customer?

● Simple AD
● Any of these options are acceptable as long as they configured correctly for 1,000 customers.
● AWS Directory Service for Microsoft Active Directory (Enterprise Edition)
✓ AD Connector
Explanation:-AD Connector helps connecting your on-premises Microsoft Active Directory to the AWS cloud.

Q30)

You have created a temporary application that accepts image uploads, stores them in S3, and records information about the image in RDS.

After building this architecture and accepting images for the duration required, it's time to delete the CloudFormation template.

However, your manager has informed you that for archival reasons the RDS data needs to be stored and the S3 bucket with the images needs to remain.

Your manager has also instructed you to ensure that the application can be restored by a CloudFormation template and run next year during the same period.

Knowing that when a CloudFormation template is deleted, it will remove the resources it created, what is the best method to achieve the desired goals? Choose the correct answer from the options below

● Set the DeletionPolicy on the S3 resource to snapshot and the DeletionPolicy on the RDS resource to snapshot.
● For both the RDS and S3 resource types on the CloudFormation template, set the DeletionPolicy to Retain
✓ Set the DeletionPolicy on the S3 resource declaration in the CloudFormation template to retain, set the RDS resource declaration DeletionPolicy to snapshot.
Explanation:-It correctly sets the DeletionPolicy of retain on S3 bucket and snapshot on RDS instance. More information on DeletionPolicy on CloudFront DeletionPolicy options include: Retain: You retain the resource in the event of a stack deletion. Snapshot: You get a snapshot of the resource before it's deleted. This option is available only for resources that support snapshots. Delete: You delete the resource along with the stack. This is the default outcome if you don't set a DeletionPolicy. To keep or copy resources when you delete a stack, you can specify either the Retain or Snapshot policy options. With the DeletionPolicy attribute, you can preserve or (in some cases) backup a resource when its stack is deleted. You specify a DeletionPolicy attribute for each resource that you want to control. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default.
● Enable S3 bucket replication on the source bucket to a destination bucket to maintain a copy of all the S3 objects, set the deletion policy for the RDS instance to snapshot.

Q31)

You work for a large university that has grown its AWS infrastructure significantly over the last few years, and consequently, the IT department has hired four new AWS System Administrators who will each manage a different Availability Zone in your infrastructure. You have 4 AZs.

You have been given the task of providing access to the new staff, to be able to launch and manage instances in their zone only, and should not be able to modify any of the other administrators' zones.

Which of the following options is the best solution to accomplish your task? Choose an answer from the options below

✓ Create a VPC with four subnets, and allow access to each subnet for the individual IAM user.
● Create four IAM users and four VPCs, allow each IAM user to have access to separate VPCs.
● Create an IAM user, and allow them permission to launch an instance of a different size only.
● Create four AWS accounts, and give each user access to a separate account.

Q32)

In an attempt to cut costs your accounts manager has come to you and tells you that he thinks that if the company starts to use consolidated billing that it will save some money.

He also wants the billing set up in such a way that it is relatively simple, and it gives insights into the environment regarding utilization of resources.

Which of the following consolidated billing setups would satisfy your account manager's needs? Choose two answers from the options below

● Use one master account and no linked accounts.
✓ Use one account but multiple VPCs to break out environments.
Explanation:-VPC helps you seggregate and organize your resources as per the functionality or domain, thus enabling the account owner to get the insight of the costing of the resources within the logical grouping of the resources. e.g. If an organization has separate VPC for each department - Finance, Development, Sales etc. It will be convinient to get the billing details per department.
As having linked account would enable the accounts manager to leverage the Consolidated Billing for multiple AWS accounts. With Consolidated Billing, you can see a combined view of AWS charges incurred by all accounts, as well as get a cost report for each account assicuated with your payer account.
✓ Use one master account and many linked accounts.
Explanation:-VPC helps you seggregate and organize your resources as per the functionality or domain, thus enabling the account owner to get the insight of the costing of the resources within the logical grouping of the resources. e.g. If an organization has separate VPC for each department -

Finance, Development, Sales etc. It will be convinient to get the billing details per department.

As having linked account would enable the accounts manager to leverage the Consolidated Billing for multiple AWS accounts. With Consolidated Billing, you can see a combined view of AWS charges incurred by all accounts, as well as get a cost report for each account assicuated with your payer account.

● Use roles for IAM account simplicity across multiple AWS linked accounts.

Q33)

A company is managing a customer's application which currently includes a three-tier application configuration. The first tier manages the web instances and is configured in a public subnet. The second layer is the application layer.

As part of the application code, the application instances upload large amounts of data to Amazon S3.

Currently, the private subnets that the application instances are running on have a route to a single NAT t2.micro NAT instance.

The application, during peak loads, becomes slow and customer uploads from the application to S3 are not completing and taking a long time.

Which steps might you take to solve the issue using the most cost-efficient method? Choose the correct answer from the options below

● Launch an additional NAT instance in another subnet and replace one of the routes in a subnet to the new instance

● Increase the NAT instance size; network throughput increases with an increase in instance size

✓ Create a VPC S3 endpoint

Explanation:-With S3 Endpoint, the VPC can privately and securely connect to the S3 buckets. No additional infrastructure provisioning such as NAT or Gateway is needed, hence saving the cost.

● Configure Auto Scaling for the NAT instance in order to handle increase in load

Q34)

You are excited that your company has just purchased a Direct Connect link from AWS as everything you now do on AWS should be much faster and more reliable.

Your company is based in Sydney, Australia so obviously, the Direct Connect Link to AWS will go into the Asia Pacific (Sydney) region.

Your first job after the new link purchase is to create a multi-region design across the Asia Pacific(Sydney) region and the US West (N. California) region.

You soon discover that all the infrastructure you deploy in the Asia Pacific(Sydney) region is extremely fast and reliable, however, the infrastructure you deploy in the US West(N. California) region is much slower and unreliable.

Which of the following would be the best option to make the US West(N. California) region a more reliable connection? Choose the correct answer from the options below

● Create a private virtual interface to the Asia Pacific region's public end points and use VPN over the public virtual interface to protect the data.

● Create a private virtual interface to the US West region's public end points and use VPN over the public virtual interface to protect the data

✓ Create a public virtual interface to the US West region's public end points and use VPN over the public virtual interface to protect the data.

Explanation:-It creates a public virtual interface to the US West region which allows you to connect to the Asia Pacific region. Also, it uses secure VPN connection over the public virtual interface for the data protection.

● Create a public virtual interface to the Asia Pacific region's public end points and use VPN over the public virtual interface to protect the data.

Q35)

A company has a library of on-demand MP4 files needing to be streamed publicly on their new video webinar website.

The video files are archived and are expected to be streamed globally, primarily on mobile devices.

Given the requirements what would be the best architecture for the company to design?

● Provision streaming EC2 instances which use S3 as the source for the HLS on-demand transcoding on the servers. Provision a new CloudFront streaming distribution with the streaming server as the origin.

● Upload the MP4 files to S3 and create an Elastic Transcoder job that transcodes the MP4 source into HLS chunks. Store the HLS output in S3 and Configure the Amazon CloudFront distribution with a streaming option to stream the video contents.

✓ Upload the MP4 files to S3 and create an Elastic Transcoder job that transcodes the MP4 source into HLS chunks. Store the HLS output in S3 and create a media streaming CloudFront distribution with download option to serve the HLS files to end users.

Explanation:-It (a) it uses Elastic Transcoder for transcoding the videos to different formats, (b) it uses CloudFront distribution with download option for streaming the on demand videos using HLS on any mobile, and (c) it uses S3 as origin, so keeps the cost low.

● Provision streaming EC2 instances which use S3 as the source for the HLS on-demand transcoding on the servers. Provision a new CloudFront download distribution with the WOWZA streaming server as the origin.

Q36)

A company has a Redshift cluster for petabyte-scale data warehousing.

The data within the cluster is easily reproducible from additional data stored on Amazon S3.

The company wants to reduce the overall total cost of running this Redshift cluster.

Which scenario would best meet the needs of the running cluster, while still reducing total overall ownership cost of the cluster? Choose the correct answer from the options below

● Enable automated snapshots but set the retention period to a lower number to reduce storage costs

● Instead of implementing automatic daily backups, write a CLI script that creates manual snapshots every few days. Copy the manual snapshot to a secondary AWS region for disaster recovery situations.

✓ Disable automated and manual snapshots on the cluster

Explanation:-Taking any of automated and manual snapshots is unnecessary as the cluster can easily be restored via the data stored in S3. Hence, once the snapshot taking is disabled, the cost would be lowered.

● Implement daily backups, but do not enable multi-region copy to save data transfer costs.

Q37)

While implementation of cost-cutting measurements in your organization, you have been told that you need to migrate some of your existing resources to another region.

The first task you have been given is to copy all of your Amazon Machine Images from Asia Pacific (Sydney) to US West (Oregon).

One of the things that you are unsure of is how the PEM keys on your Amazon Machine Images need to be migrated.

Which of the following best describes how your PEM keys are affected when AMIs are migrated between regions? Choose the correct answer from the options below

● The PEM keys will also be copied across so you don't need to do anything except launch the new instance.

● The PEM keys will also be copied across; however, they will only work for users who have already accessed them in the old region. If you need new users to access the instances then new keys will need to be generated.

✓ The PEM keys will not be copied to the new region but the authorization keys will still be in the operating system of the AMI. You need to ensure when the new AMI is launched that it is launched with the same PEM key name.

Explanation:-The authorization key is included in the AMI, hence copied across the region; however, the PEM keys are not copied; hence, need to be imported explicitly. See the AWS Console option for importing the PEM key.

● Neither the PEM key nor the authorized key is copied and consequently you need to create new keys when you launch the new instance.

Q38)

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

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

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

● Create an 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 that stores documents and in that policy grant access to only CloudFront.

● 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.

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.

Q39)

There are 2 companies that have their own AWS accounts.

How can they connect to a central VPC for identity validation?

How would you best design this solution? Choose an answer from the options below

● Create an OpenVPN instance in central VPC and establish an IPSec tunnel between VPCs.

● Migrate each VPC resources to the central VPC using migration tools such as Import/Export, Snapshot, AMI Copy, and S3 sharing.

✓ Create a VPC peering connection with the central VPC

Explanation:-VPC peering allows the resources in peer VPCs to communicate with each other and in this case, can validate the identities of the resources. See the image below. Also, VPCs from different regions can be peered as well (Inter-Region VPC Peering).

● Create a Direct Connect connection from each VPC endpoint to the central VPC.

Q40)

An auditor needs access to logs that record all the API events on AWS.

The auditor only needs read-only access to the log files and does not need access to each AWS account.

The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts.

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

✓ Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket in the primary account and grant the auditor access to that single bucket in the primary account.

Explanation:-It delivers the logs pertaining to different AWS accounts to a single S3 bucket in the primary account and grants the auditor the access to it.

● Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.

● Configure the CloudTrail service in each AWS account, and make the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary IAM account that can assume a read-only role in the secondary AWS accounts.

● Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary accounts. Then grant the auditor access to the S3 bucket that receives the CloudTrail log files.

Q41)

The company you work for has a huge amount of infrastructure built on AWS. However, there has been some concerns recently about the security of this infrastructure, and an external auditor has been given the task of running a thorough check of all of

your company's AWS assets.

The auditor will be in the USA while your company's infrastructure resides in the Asia Pacific (Sydney) region on AWS. Initially, he needs to check all of your VPC assets, specifically, security groups and NACLs You have been assigned the task of providing the auditor with a login to be able to do this.

Which of the following would be the best and most secure solution to provide the auditor with so he can begin his initial investigations? Choose the correct answer from the options below

● Give him root access to your AWS Infrastructure, because he is an auditor he will need access to every service.
● Create an IAM user with full VPC access but set a condition that will not allow him to modify anything if the request is from any IP other than his own.
● Create an IAM user tied to an administrator role. Also provide an additional level of security with MFA.
✓ Create an IAM Role with the read only permissions to access the AWS VPC infrastructure and assign that role to the auditor.
Explanation:-IAM Role gives just the minimum required permissions (read-only) to audit the VPC infrastructure to the auditor.

Q42)

A company runs their current application entirely on-premise. However, they are expecting a big boost in traffic and need to figure out a way to decrease the load to handle the scale.

Unfortunately, they cannot migrate their application to AWS in the period required.

What could they do with their current on-premise application to help offload some of the traffic and scale to meet the demand expected in 24 hours in a cost-effective way? Choose the correct answer from the options below.

✓ Create a CloudFront CDN, enable query string forwarding and TTL of zero on the origin. Offload the DNS to AWS to handle CloudFront CDN traffic but use on-premise load balancers as the origin.
Explanation:-CloudFront - which is an AWS managed - is a highly available, scalable service that can use the on-premises server as the origin. By setting the TTL to 0, the content will be delivered from the origin as soon as it gets changed.
● Deploy OpsWorks on-premise to manage the instance in order to configure on-premise auto scaling to meet the demand.
● Duplicate half your web infrastructure on AWS, offload the DNS to Route 53 and configure weighted based DNS routing to send half the traffic to AWS .
● Upload all static files to Amazon S3 and create a CloudFront distribution serving those static files.

Q43)

You have two different groups to analyze data of a petabyte-scale data warehouse using Redshift. Each query issued by the first group takes approximately 1-2 hours to analyze the data while the second group's queries only take between 5-10 minutes to analyze data.

You don't want the second group's queries to wait until the first group's queries are finished.

You need to design a solution so that this does not happen.

Which of the following will be the best and cheapest solution to solve this dilemma? Choose an answer from the options below

● Create a read replica of Redshift and run the second team's queries on the read replica.
✓ Create two separate workload management groups and assign them to the respective groups.
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.
● Start another Redshift cluster from a snapshot for the second team if the current Redshift cluster is busy processing long queries.
● Pause the long queries when necessary and resume them when no query is running.

Q44)

You have created a mobile application that serves data stored in an Amazon DynamoDB table.

Your primary concern is scalability of the application and being able to handle millions of visitors and data requests.

As part of your application, the customer needs access to the data located in the DynamoDB table.

Given the application requirements, what would be the best method to design the application? Choose the correct answer from the options below

● Configure an on-premise AD server utilizing SAML 2.0 to manage the application users inside the on-premise AD server and write code that authenticates against the LD serves. Grant a role assigned to the STS token to allow the end-user to access the required data in the DynamoDB table.
● Let the users sign into the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWith API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in JavaScript and host the JavaScript interface in an S3 bucket.
● Let the users sign into the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWithWebIdentity API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in a server-side language using the AWS SDK and host the application in an S3 bucket for scalability.
✓ Let the users sign in to the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWithWebIdentity API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in JavaScript and host the JavaScript interface in an S3 bucket.
Explanation:-The AssumeRolewithWebIdentity returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider.

Q45)

A company is running data application on-premise that requires large amounts of data to be transferred to a VPC containing

EC2 instances in an AWS region.

The company is concerned about the total overall transfer costs required for this application and is potentially not going deploy a hybrid environment for the customer-facing part of the application to run in a VPC.

Given that the data transferred to AWS is new data every time, what suggestions could you make to the company to help reduce the overall cost of data transfer to AWS? Choose the correct answer from the options below

● Suggest using AWS import/export to transfer the TBs of data while synchronizing the new data as it arrives.
● Suggest leaving the data required for the application on-premise and use a VPN to query the on-premise database data from EC2 when required.
✓ Suggest provisioning a Direct Connect connection between the on-premise data center and the AWS region.
Explanation:-(a) since it is a dedicated connection from on-premises data center to AWS, it takes out the unpredictable nature of the internet out of the equation, and (2) due to the high bandwidth availability, Direct Connect would most probably transfer the large amount of data quickly compared to VPN connection. Hence, it may well save the cost for the customer.
● Provision a VPN connection between the on-premise data center and the AWS region using the VPN section of a VPC.

Q46)

You have a legacy application running that uses an m4.large instance size and cannot scale with Auto Scaling, but only has peak performance 5% of the time.

This is a huge waste of resources and money so your Senior Technical Manager has set you the task of trying to reduce costs while still keeping the legacy application running as it should.

Which of the following will best accomplish the task your manager has assigned you? Choose the correct answer from the options below:

● Use two t2.nano instances that have single Root I/O Virtualization.
● Use a C4.large instance with enhanced networking.
✓ Use a T2 burstable performance instance.
Explanation:-The AWS documentation clearly indicates using T2 EC2 instance types for those instances which don't use CPU that often.
● Use t2.nano instance and add spot instances when they are required.

Q47)

Your supervisor gave you brief of a client who needs a web application set up on AWS.

The most important requirement is that MySQL must be used as the database, and this database must not be hosted in the public cloud, rather at the client's data center due to security risks.

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

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

Q48)

You have been tasked with creating file level restore on your EC2 instances.

You already have the access to all the frequent snapshots of the EBS volume.

You need to be able to restore an individual lost file on an EC2 instance within 15 minutes of a reported loss of information.

The acceptable RPO is several hours.

How would you perform this on an EC2 instance? Choose an answer from the options below

● Enable auto snapshots on Amazon EC2 and restore the EC2 instance upon single file failure
● Turn off the frequent snapshots of EBS volumes. Create a volume from an EBS snapshot, attach the EBS volume to the EC2 instance at a different mount location, cutover the application to look at the new backup volume and remove the old volume
✓ Create a volume from an EBS snapshot, attach the EBS volume to the EC2 instance at a different mount location, browse the file system to the file that needs to be restored on the new mount, copy from the new volume to the backup volume
Explanation:-It mounts the EBS snapshot - that contains the file - as a volume and copies the file to the already attached volume. This way, the already attached volume always stays up-to-date. Once the file is copied, the volume - that was attached for copying the file - can be removed.
● Setup a cron that runs aws s3 cp on the files and copy the files from the EBS volume to S3

Q49)

After having created a VPC with CIDR block 10.0.0.0/24 and launching it as a working network, a few weeks later you decide that it is too small and you want to make it larger.

Which of the below options would accomplish this successfully? Choose an answer from the options below

✓ Expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC
Explanation:-You can expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC.
● Re-allocate the VPC with CIDR 10.0.0.0/16

● You cannot change a VPC's size. To change the size of a VPC you must terminate your existing VPC and create a new one.
● Peer with another VPC with CIDR 10.0.0.0/28 to this VPC. This will ensure that the IPs do not overlap.

Q50)

An employee keeps terminating EC2 instances on the production environment.

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

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

✓ Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.
Explanation:-To stop the users from manipulating any AWS resources, you can either create the applicable (allow/deny) resource level permissions and apply them to those users, or create an individual or group policy which explicitly denies the action on that resource and apply it to the individual user or the group.

(a) identifies the instances with proper tag, and (b) creates a resource level permission and explicitly denies the user the terminate option.
(a) identifies the instances with proper tag, and (b) creates a policy with explicit deny of terminating the instances and applies that policy to the group which contains the employees (who are not supposed to have the access to terminate the instances).
● Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
✓ Tag the instance with a production-identifying tag and modify the employees group to allow only start, stop, and reboot API calls and not the terminate instance call.
Explanation:-To stop the users from manipulating any AWS resources, you can either create the applicable (allow/deny) resource level permissions and apply them to those users, or create an individual or group policy which explicitly denies the action on that resource and apply it to the individual user or the group.

(a) identifies the instances with proper tag, and (b) creates a resource level permission and explicitly denies the user the terminate option.
(a) identifies the instances with proper tag, and (b) creates a policy with explicit deny of terminating the instances and applies that policy to the group which contains the employees (who are not supposed to have the access to terminate the instances).
● Modify the IAM policy on the user to require MFA before deleting EC2 instances