Answer Sheet

Q1)

You are launching your first ElastiCache cache cluster, and start using Memcached.

Which of the following is NOT a key features of Memcache. Choose the correct answer from the options below

✓ You use more advanced data types, such as lists, hashes, and sets.

Explanation:-It is Redis, not Memcached,which supports advanced/complexdata types such as strings, hashes, lists, sets, sorted sets, and bitmaps.

● You need as simple a caching model as possible.

● Object caching is your primary goal to offload your database.

● You need the ability to scale your cache horizontally as you grow.

Q2)

You're consulting for a company that is migrating its legacy application to the AWS cloud. In order to apply high availability, you've decided to implement Elastic Load Balancer and Auto Scaling services to serve traffic to this legacy application.

The legacy application is not a standard HTTP web application but is a custom application with custom codes that is run internally for the employees of the company you are consulting.

The ports required to be open are port 80 and port 8080.

Which listener configuration would you create? Choose an answer from the options below

✓ Configure the load balancer with the following ports: TCP:80 and TCP:8080 and the instance protocol to TCP:80 and TCP:8080

Explanation:-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.

● 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

Q3)

The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network.

You can have multiple sets of DHCP options, but you can associate only one set of DHCP options with a VPC at a time.

You have just created your first set of DHCP options, associated it with your VPC but now realize that you have made an error in setting them up and you need to change the options.

Which of the following options do you need to take to achieve this? Choose the correct answer from the options below

● 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 can modify the options from the console or the CLI.

✓ You must create a new set of DHCP options and associate them with your VPC.

Explanation:-Once you create a set of DHCP options, you cannot modify them. You must create a new set of DHCP options and associate it with your VPC.

Q4)

Your application is having a very high traffic, so you have enabled autoscaling in the multi-availability zone to suffice the needs of your application but you observe that one of the availability zones is not receiving any traffic.

What can be wrong here?

● Autoscaling can be enabled for multi AZ only in north Virginia region

✓ Availability zone is not added to Elastic load balancer

● Instances need to manually added to availability zone

● Autoscaling only works for single availability zone

Q5) Which of the below-mentioned options is the best for on-premise users to manage AWS resources from the AWS console, if you want to re-use the existing on-premise credentials?

● Use your on-premises SAML 2.0-compliam identity provider (IDP) to retrieve temporary security credentials to enable members to sign in to the AWS Management Console.

● Use web Identity Federation to retrieve AWS temporary 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 grant the members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.

Explanation:-This scenario has two requirements: (a) temporary access to AWS resources be given to certain users or application (NOC members in this case), and (b) you are not supposed to create new IAM users for the NOC members to log into AWS console. This scenario is handled by a concept named "Federated Access". Read this for more information on federated access: https://aws.amazon.com/identity/federation/ . Read this article for more information on how to establish the federated access to the AWS resources: https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-active-directory-user-attributes/ Option A is incorrect because OAuth 2.0 is not applicable in this scenario as we are not using Web Identity Federation as it is used with public identity providers such as Facebook, Google etc. Option B is incorrect because we are not using Web Identity Federation as it is used with public identity providers such as Facebook, Google etc. Option C is CORRECT because (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. Option D is incorrect because, even though it uses SAML 2.0 identity provider, one of the requirements is not to let users sign in to AWS console using any security credentials. The correct answer is: 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 OAuth 2.0 to retrieve temporary AWS security credentials to enable your members to sign in to the AWS Management Console.

Q6)

A company needs to configure a NAT instance for its internal AWS applications to be able to download patches and package software.

Currently, they are running a NAT instance that is using the floating IP scripting configuration to create fault tolerance for the NAT.

The NAT instance needs to be built with fault tolerance in mind.

What is the best way to configure the NAT instance with fault tolerance? Choose the correct answer from the options below:

● Create one NAT instance in a public subnet; create a route from the private subnet to the NAT instance

● Create two NAT instances in a public subnet; create a route from the private subnet to each NAT instance for fault tolerance.

● Create two NAT instances in two separate private subnets.

✓ Create two NAT instances in two separate public subnet; create a route from the private subnet to each NAT instance for fault tolerance

Explanation:-Because you should place two NAT instances in two separate public subnets, and create route from instances via each NAT instance for achieving fault tolerance.

Q7) What could be the possible cause of an HTTP Status Code 502 error code when using CloudFront. Choose an answer from the options below

✓ Could not connect to the origin server

● None of these

● Cloudfront service is down

Q8)

You're migrating an existing application to the AWS cloud. The application will be primarily using EC2 instances.

This application needs to be built with the highest availability architecture available.

The application currently relies on hardcoded hostnames for intercommunication between the three tiers.

You've migrated the application and configured the multi-tiers using the internal Elastic Load Balancer for serving the traffic.

The load balancer hostname is demo-app.us-east-1.elb.amazonaws.com.

The current hard-coded hostname in your application used to communicate between your multi-tier application is demolayer.example.com.

What is the best method for architecting this setup to have as much high availability as possible? Choose the correct answer from the options below

● Create an environment variable passed to the EC2 instances using user-data with the ELB hostname, demo-app.us-east-1.elb.amazonaws.com.

✓ Create a private resource record set using Route 53 with a hostname of demolayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com

Explanation:-It creates an internal ALIAS record set where it defines the mapping between the hard-coded host name and the ELB host name that is to be used.

● Create a public resource record set using Route 53 with a hostname of demolayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com

● Add a cname record to the existing on-premise DNS server with a value of demo-app.us-east-1.elb.amazonaws.com. Create a public resource record set using Route 53 with a hostname of applayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com.

Q9)

A company is building an AWS Cloud Environment for a financial regulatory firm. Part of the requirements is being able to monitor all changes in an environment and all traffic sent to and from the environment.

What suggestions would you make to ensure all the requirements for monitoring the financial architecture are satisfied? Choose the 2 correct answers from the options below

● 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 system, such as Palo Alto Networks, that monitors, filters, and alerts of all potential hazard traffic leaving the VPC.

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.

✓ 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.

Q10)

An application has multiple components. The single application and all the components are hosted on a single EC2 instance (without an ELB) in a VPC.

You have been told that this needs to be set up with two separate SSLs for each component.

Which of the following would best achieve the setting up of the two separate SSLs while using still only using one EC2 instance? Choose the correct answer from the options below

● Create an EC2 instance which has multiple subnets attached to it and each will have a separate IP address.
● Create an EC2 instance which has both an ACL and the security group attached to it and have separate rules for each IP address.
● Create an EC2 instance with a NAT address.
✓ Create an EC2 instance which has multiple network interfaces with multiple elastic IP addresses.
Explanation:-It can be useful to assign multiple IP addresses to an instance in your VPC to do the following: (1) Host multiple websites on a single server by using multiple SSL certificates on a single server and associating each certificate with a specific IP address. (2) Operate network appliances, such as firewalls or load balancers, that have multiple IP addresses for each network interface. (3) Redirect internal traffic to a standby instance in case your instance fails, by reassigning the secondary IP address to the standby instance.
As mentioned above, if you have multiple elastic network interfaces (ENIs) attached to the EC2 instance, each network IP can have a component running with a separate SSL certificate.

Q11)

A third party auditor is being brought in to review security processes and configurations for all of a company's AWS accounts.

Currently, the company does not use any on-premise identity provider. Instead, they rely on IAM accounts in each of their AWS accounts.

The auditor needs read-only access to all AWS resources for each AWS account.Given the requirements, what is the best security method for architecting access for the security auditor?

Choose the correct answer from the options below

● Create a custom identity broker application that allows the auditor to use existing Amazon credentials to log into the AWS environments.
● Create an IAM user for each AWS account with read-only permission policies for the auditor, and disable each account when the audit is complete.
● Configure an on-premise AD server and enable SAML and identify federation for single sign-on to each AWS account.
✓ Create an IAM role with read-only permissions to all AWS services in each AWS account. Create one auditor IAM account and add a permissions policy that allows the auditor to assume the ARN role for each AWS account that has an assigned role.
Explanation:-It creates an IAM Role which has all the necessary permission policies attached to it which allows the auditor to assume the appropriate role while accessing the resources.

Q12)

There are currently multiple applications hosted in a VPC. During monitoring, it has been noticed that multiple port scans are coming in from a specific IP Address block.

The internal security team has requested that all offending IP Addresses be denied for the next 24 hours.

Which of the following is the best method to quickly and temporarily deny access from the specified IP Addresses?

● Modify the Windows Firewall settings on all AMI's that your organization uses in that VPC to deny access from the IP address block
● Add a rule to all of the VPC Security Groups to deny access from the IP Address block
✓ Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block
Explanation:-A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. Option A and D are incorrect because (a)it will only work for windows-based instances, and (b)better approach is to block the traffic at the subnet layer via NACL rather than instance layer (windows firewall). Option B is CORRECT because the best way to allow or deny IP address-based access to the resources in the VPC is to configure rules in the Network access control list(NACL) which are applied at the subnet level. Option C is incorrect because (a)you cannot explicitly deny access to particular IP addresses via security group, and (b)better approach is to block the traffic at the subnet layer via NACL rather than instance layer (security group). For more information on network ACL's please refer to the below link http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html The correct answer is: Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block
● Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block

---

Q13)

There is a requirement to migrate 50TB of data to AWS. There is a restriction of the time to migrate the data and there is a limitation of only a 100MBit line to the AWS Cloud.

What is the best solution to use to migrate the data to the cloud?

● Amazon S3
✓ AWS Snowball
Explanation:-When you have a limitation on the bandwidth, the best option is to use the Snowball option. AWS Snowball is a service that accelerates transferring large amounts of data into and out of AWS using physical storage appliances, bypassing the Internet. Each AWS Snowball appliance type can transport data at faster-than internet speeds. This transport is done by shipping the data in the appliances through a regional carrier. To get more information on Amazon snowball, please refer to the link https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html Refer to the blog given below which gives a case study of comparing the price of transferring the data via S3 Accelerated Transfer and Snowball: https://www.cloudberrylab.com/blog/amazon-s3-transfer-acceleration-vs-amazon-snowball/ The correct answer is: AWS Snowball
● Amazon Storage Gateway
● Amazon Direct Connect

Q14)

A legacy application is being migrated to AWS. It works on the TCP protocol.

There is a requirement to ensure scalability of the application and also ensure that records of the client IP using the application are recorded.

Which of the below-mentioned steps would you implement to fulfill the above requirement?

● Use an ELB with a TCP Listener and Cross-Zone Load Balancing enabled, two application servers in different AZs.
● Use Route 53 with Latency Based Routing enabled to distribute load on two or more application servers in different AZs.
● Use Route 53 Alias Resource Record to distribute load on two application servers in different AZs.
✓ Use an ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two or more 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. This option is CORRECT because it implements the proxy protocol and uses ELB with TCP listener.

Q15)

There is a requirement for an application hosted on a VPC to access the On-premise LDAP server.

The VPC and the on-premise location are connected via an IPSec VPN.

Which of the below are the right options for the application to authenticate each user? Choose 2 options from the below:

✓ Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate AWS service.
Explanation:-There are two architectural considerations here: (1) The users must be authenticate 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. An example diagram of how this works from the AWS documentation is given below. 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 to assume that IAM role. The application can use the temporary credentials to access any AWS resources., Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate AWS service.
● Develop an identity broker that authenticates against IAM security Token service 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.
✓ 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 to assume that IAM role. The application can use the temporary credentials to access any AWS resources.
Explanation:-There are two architectural considerations here: (1) The users must be authenticate 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. An example diagram of how this works from the AWS documentation is given below. 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 to assume that IAM role. The application can use the temporary credentials to access any AWS resources., Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate AWS service.

Q16)

There is a requirement to carry out the backup of an Oracle RAC cluster which is currently hosted on the AWS public cloud.

How can this be achieved?

● Enable automated backups on the RDS RAC cluster; enable auto snapshot copy to a backup region to reduce RPO and RTO.
● Enable Multi-AZ failover on the RDS RAC cluster to reduce the RPO and RTO in the event of disaster or failure.
✓ Create a script that runs snapshots against the EBS volumes to create backups and durability.
Explanation:-Currently, Oracle Real Application Cluster (RAC) is not supported as per the AWS documentation. However, you can deploy scalable RAC on Amazon EC2 using the recently-published tutorial and Amazon Machine Images (AMI). So, in order to take the backups, you need to take the backup in the form of EBS volume snapshots of the EC2 that is deployed for RAC. For more information on Oracle RAC on AWS, please visit the below URL: https://aws.amazon.com/about-aws/whats-new/2015/11/self-managed-oracle-rac-on-ec2/ https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/ https://aws.amazon.com/blogs/database/amazon-aurora-as-an-alternative-to-oracle-rac/ The correct answer is: Create a script that runs snapshots against the EBS volumes to create backups and durability.
● Create manual snapshots of the RDS backup and write a script that runs the manual snapshot

---

Q17)

Your company has a lot of GPU intensive workloads. Also, these workloads are part of a process in which some steps need manual intervention.

Which of the below options works out for the above-mentioned requirement?

● Use AWS data Pipeline to manage the workflow. Use auto-scaling group of C3 with SR-IOV (Single Root I/O virtualization).

● Use Amazon Simple Workflow (SWF) to manage the workflow. Use an autoscaling group of C3 instances with SR-IOV (Single Root I/O Virtualization).
✓ Use Amazon Simple Workflow (SWF) to manage the workflow. Use an autoscaling group of G2 instances in a placement group.
Explanation:-Tip: Whenever the scenario in the question mentions about high graphical processing servers with low latency networking, always think about using G2 instances. And, when there are tasks involving human intervention, always think about using SWF.
● Use AWS Data Pipeline to manage the workflow. Use an auto-scaling group of G2 instances in a placement group.

Q18)

A company has the requirement to analyze the clickstreams from a web application.

Which of the below options will fulfill this requirement?

● Publish web clicks by session to an Amazon SQS queue and periodically drain these events to Amazon RDS. Then, analyze with SQL
● Write click events directly to Amazon Redshift and then analyze with SQL
✓ 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 The below diagrams from the aws documentation shows how you can create custom streams in Amazon Kinesis. For more information on Kinesis, please visit the below link: http://docs.aws.amazon.com/streams/latest/dev/introduction.html The correct answer is: Push web clicks by session to Amazon Kinesis and analyze behavior using Kinesis workers
● Log clicks in weblogs by URL and store it in Amazon S3, and then analyze with Elastic MapReduce

Q19)

A company currently has an on-premise location connecting to a VPC.

The company wants to have a dedicated network connection from the on-premise location to the VPC.

Choose the correct answer from the below options which would help to fulfill the above requirement

● Use a hardware VPN to connect both locations.
✓ Suggest provisioning a Direct Connect connection between the on-premise data center and the AWS region.
Explanation:-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. Hence, option B is CORRECT. Option A, C, and D all are incorrect because VPN connectivity is done over the internet, not a dedicated network connection. For more information on AWS direct connect, just browse to the below URL: https://aws.amazon.com/directconnect/ The correct answer is: Suggest provisioning a Direct Connect connection between the on-premise data center and the AWS region.
● Provision a VPN connection between the on-premise data center and the AWS region using the VPN section of a VPC.
● Use a software VPN to connect both locations.

Q20)

A custom script needs to be passed to a new Amazon Linux instances created in your Auto Scaling group.

Which feature allows you to accomplish this?

● EC2Config service
✓ User data
Explanation:-When you configure an instance during creation, you can add custom scripts to the User data section. So in Step 3 of creating an instance, in the Advanced Details section, we can enter custom scripts in the User Data section. The below script installs Perl during the instance creation of the EC2 instance. For more information on user data please refer to the URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html The correct answer is: User data
● IAM roles
● AWS Config

Q21) What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment if the primary DB instance fails?

● A new DB instance is created in the standby availability zone.
● The primary RDS (Relational Database Service) DB instance reboots and remains as primary.
● The IP address of the primary DB instance is switched to the standby DB instance.
✓ The canonical name record (CNAME) is changed from primary to standby.

Q22)

An organization is planning to use AWS for their production roll out. The organization wants to implement automation for deployment such that it will automatically create a LAMP stack, download the latest PHP installable from S3 and setup the ELB.

Which of the below mentioned AWS services meets the requirement for making an orderly deployment of the software?

● AWS Cloudfront
✓ AWS Elastic Beanstalk
Explanation:-The Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. We can simply upload code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health

monitoring. Meanwhile we can retain full control over the AWS resources used in the application and can access the underlying resources at any time.

● AWS Cloudformation
● AWS DevOps

Q23) Which section in your CloudFormation template would you modify to fire up different instance sizes based off of environment type (Dev/Staging/Production)? Choose the correct answer from below options:

● Outputs
● Resources
● Mappings
✓ Conditions

Explanation:-The optional Conditions section includes statements that define when a resource is created or when a property is defined. For example, you can compare whether a value is equal to another value. Based on the result of that condition, you can conditionally create resources. If you have multiple conditions, separate them with commas. For more information on Cloudformation conditions please visit the below link http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/conditions-section-structure.html The correct answer is: Conditions

Q24)

You have an application running on an EC2 instance which allows 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.

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 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 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.

● 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.

Q25)

Your company's on-premises content management system has the following architecture.

It has an Application Tier hosted on IIS.

The database Tier is MySQL database.

This is regularly backed up to Amazon Simple Storage Service (S3) using the a custom backup utility.

The static Content is stored on a 512GB gateway stored Storage Gateway volume attached to the application server via the iSCSI interface

Which AWS based disaster recovery strategy will give you the best RTO?

● Deploy the MySQL database and the IIS app server on EC2. Restore the backups from Amazon S3. Restore the static content from an AWS Storage Gateway-VTL running on Amazon EC2. Deploy the MySQL database and the IIS app server on EC2. Restore the backups from Amazon S3. Restore the static content from an AWS Storage Gateway-VTL running on Amazon EC2.
● Deploy the MySQL database and the IIS app server on EC2. Restore the MySQL backups from Amazon S3. Restore the static content by attaching an AWS Storage Gateway running on Amazon EC2 as an iSCSI volume to the IIS EC2 server.
✓ Deploy the MySQL database and the IIS app server on EC2. Restore the backups from Amazon S3. Generate an EBS volume of static content from the Storage Gateway and attach it to the IIS EC2 server.
● Deploy the MySQL database on RDS. Deploy the IIS app server on EC2. Restore the backups from Amazon Glacier. Generate an EBS volume of static content from the Storage Gateway and attach it to the IIS EC2 server.

Q26)

You currently have developers who have access to your production AWS account? There is a concern raised that the developers could potentially delete the production-based EC2 resources.

Which of the below options could help alleviate this concern? Choose 2 options from the below:

● Modify the IAM policy on the developers 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. Option A is CORRECT because it (a) identifies the instances with proper tag, and (b) creates a resource level permission and explicitly denies the user the terminate option. Option B is CORRECT because it (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). Option C and D are incorrect because MFA is an additional layer of security given to the users for logging into AWS and accessing the resources. However, either enabling or disabling MFA cannot prevent the users from performing resource level actions. More information on Tags Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define. For more information on tagging AWS resources please refer to the below URL http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html The correct answers are: Tag the production instances with a production-identifying tag and add resource-level permissions to the developers with an explicit deny on the terminate API call to instances with the production tag., Tag the instance with a production-identifying tag and modify the employees group to allow only start, stop, and reboot API calls and not the terminate instance call.

✓ Tag the production instances with a production-identifying tag and add resource-level permissions to the developers 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. Option A is CORRECT because it (a) identifies the instances with proper tag, and (b) creates a resource level permission and explicitly denies the user the terminate option. Option B is CORRECT because it (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). Option C and D are incorrect because MFA is an additional layer of security given to the users for logging into AWS and accessing the resources. However, either enabling or disabling MFA cannot prevent the users from performing resource level actions. More information on Tags Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define. For more information on tagging AWS resources please refer to the below URL http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html The correct answers are: Tag the production instances with a production-identifying tag and add resource-level permissions to the developers with an explicit deny on the terminate API call to instances with the production tag., 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.

● Modify the IAM policy on the developers to require MFA before deleting EC2 instances

Q27)

You are designing an intrusion detection prevention (IDS/IPS) solution for a customer's web application in a single VPC.

You are considering the options for implementing IDS/IPS protection for traffic coming from the Internet.

Which of the following options would you consider? Choose 2 options from the below

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

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 which the 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. Option A is CORRECT because it implements the IDS/IPS agents on each EC2 instances in the VPC. Option B is incorrect because promiscuous mode is not supported by AWS. Option C is incorrect because ELB with SSL is does not have the intrusion detection/prevention capability. Option D is CORRECT because a reverse proxy server through which the traffic from instances inside VPC flows outside of it, has the IDS/IPS agent installed. For more information on intrusion detection systems in AWS, please refer to the below link: https://awsmedia.s3.amazonaws.com/SEC402.pdf The correct answers are: Implement IDS/IPS agents on each Instance running In VPC, Implement a reverse proxy layer in front of web servers and configure IDS/IPS agents on each reverse proxy server.

Q28)

There is a requirement to split a subnet (CIDR block - 10.0.0.0/24) into two subnets, each supporting 128 IP addresses.

Can this be done and if so, how will the allocation of IP addresses be configured? Choose the correct answer from the below options.

● This is not possible.
● One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.1.0/25 (for addresses 10.0.1.0 - 10.0.1.127).
● One subnet will use CIDR block 10.0.0.0/127 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/255 (for addresses 10.0.0.128 - 10.0.0.255).
✓ One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).

Explanation:-This is clearly given in the AWS documentation For more information on VPC and subnets please see the below link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html The correct answer is: One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).

Q29)

An application has been set up with Autoscaling and EC2 instances in multiple AZ's. When you look at the load balancer logs

you notice that EC2 instances in one of the AZ's are not receiving requests.

What can be wrong here?

● Instances need to manually added to availability zone
● Autoscaling can be enabled for multi AZ only in North Virginia region
● Autoscaling only works for single availability zone
Explanation:-In order to make sure that all the EC2 instances behind a cross-zone ELB receive the requests, make sure that all the applicable availability zones (AZs) are added to that ELB. Option A is incorrect because autoscaling can work with multiple AZs. Option B is incorrect because autoscaling can be enabled for multi AZ in any single region, not just N. Virginia. (see the image below) Option C is CORRECT because most likely the reason is that the AZ – whose EC2 instances are not receiving requests – is not added to the ELB. Option D is incorrect because instances need not be added manually to AZ (they should already be there!). More information on adding AZs to ELB When you add an Availability Zone to your load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. Load balancer nodes accept traffic from clients and forward requests to the healthy registered instances in one or more Availability Zones. For more information on adding AZ's to ELB, please refer to the below url http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-az.html The correct answer is: Availability zone is not added to Elastic load balancer
✓ Availability zone is not added to Elastic load balancer

Q30)

Your company is getting ready to do a major public announcement of a social media site on AWS. The website is running on EC2 instances deployed across multiple Availability Zones with a Multi-AZ RDS MySQL Extra Large DB Instance.

The site performs a high number of small reads and writes per second and relies on an eventual consistency model.

After comprehensive tests, you discover that there is read contention on RDS MySQL.

Which are the best approaches to meet these requirements? Choose 2 options from the below:

✓ Add an RDS MySQL read replica in each availability zone
● Increase the RDS MySQL Instance size and implement provisioned IOPS
● Implement sharding to distribute load to multiple RDS MySQL instances
Explanation:-The main point to note in this question is that there is a read contention on RDS MySQL. Your should be looking for the options which will improve upon the "read" contention issues. Hint: Always see if any of the options contain (1) caching solution such as ElastiCache, (2) CloudFront, or (3) Read Replicas. Option A is CORRECT because ElastiCache is a in-memory caching solution which reduces the load on the database and improves the read performance. Option B is incorrect because sharding does not improve read performance; however, it improves write performance, but write contention is not the issue here. Option C is incorrect because improving the instance size may improve the read performance, but only up to a specific limit. It is not a reliable solution. Option D is CORRECT because Read Replicas are used to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Hence, improving the read performance. See more information on Read Replicas and ElastiCache below. Read Replicas Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. For more information on Read Replica's, please visit the below link https://aws.amazon.com/rds/details/read-replicas/ ElastiCache Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases. For more information on Amazon ElastiCache, please visit the below link https://aws.amazon.com/elasticache/ The correct answers are: Deploy ElasticCache in-memory cache running in each availability zone, Add an RDS MySQL read replica in each availability zone
✓ Deploy ElasticCache in-memory cache running in each availability zone

---

Q31)

You have a periodic Image analysis application that gets some files. The input stream analyzes them and for each file, it writes some data to an output stream to a number of files.

The number of files in input per day is high and concentrated in a few hours of the day.

Currently, you have a server on EC2 with a large EBS volume that hosts the input data and the results it takes almost 20 hours per day to complete the process

What services could be used to reduce the elaboration time and improve the availability of the solution?

✓ Use S3 to store I/O files. The use SQS to distribute elaboration commands to a group of hosts working in parallel. Then use Auto scaling to dynamically size the group of hosts depending on the length of the SQS queue
● Use EBS with Provisioned IOPS (PIOPS) to store I/O files. Use SQS to distribute elaboration commands to a group of hosts working in parallel. Use Auto Scaling to dynamically size the group of hosts depending on the length of the SQS queue.
● Use EBS with Provisioned IOPS (PIOPS) to store I/O files. Use SNS to distribute elaboration commands to a group of hosts working in parallel and Auto Scaling to dynamically size the group of hosts depending on the number of SNS notifications
● Use S3 to store I/O files, SNS to distribute evaporation commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the number of SNS notifications
Explanation:-The scenario in this question is that (a) there any EC2 instances that need to process high number of input files, (b) currently the processing takes 20 hrs a day, which needs to be reduced, (c) the availability needs to be improved. Looking at all the option, it appears that there are two choices to be made. (1) between S3 and EBO with PIOPS, and (2) between SQS and SNS. First, let's see whether we should choose S3 or EBS with PIOPS. It appears that all the options have auto-scaling in common. i.e. there will be multiple EC2 instances working in parallel on the input data. This should reduce the overall elaboration time, satisfying one of the requirements. Since a single EBS volume cannot be attached to multiple instances, using EBS volume seems an illogical choice. Moreover, S3 provides high availability, which satisfies the other requirement. Second, SQS is a great option to do the autonomous tasks and can queue the service requests and can be scaled to meet the high demand. SNS is a mere notification service and would not hold the tasks. Hence, SQS is certainly the correct choice. Option A is CORRECT because, as mentioned above, it provides high availability, and can store the massive amount of data. Auto-scaling of EC2 instances reduces the overall processing time and SQS helps distributing the commands/tasks to the group of EC2 instances. Option B is incorrect because, as mentioned above, neither EBS nor SNS is a valid choice in this scenario. Option C is incorrect because, as mentioned above, SNS is not a valid choice in this scenario. Option D is incorrect because, as mentioned above, EBS is not a valid choice in this scenario. The correct answer is: Use S3 to store I/O files. The use SQS to distribute

elaboration commands to a group of hosts working in parallel. Then use Auto scaling to dynamically size the group of hosts depending on the length of the SQS queue

---

Q32)

You are given a task with moving a legacy application from a virtual machine running inside your datacenter to an Amazon VPC. Unfortunately, this app requires access to a number of on-premise services and no one who configured the app still works for your company.

Even worse, there's no documentation for it.

What will allow the application running inside the VPC to reach back and access its internal dependencies without being reconfigured? Choose 3 options the below:

● Entries in Amazon Route 53 that allow the Instance to resolve its dependencies' IP addresses
✓ An AWS Direct Connect link between the VPC and the network housing the internal services.
✓ An IP address space that does not conflict with the one on-premises
Explanation:-The scenario requires you to connect your on-premise server/instance with Amazon VPC. When such scenarios are presented, always think about services such as Direct Connect, VPN, and VM Import and Export as they help either connecting the instances from different location or importing them from one location to another. Option A is CORRECT because Direct Connect sets up a dedicated connection between on-premise data-center and Amazon VPC, and provides you with the ability to connect your on-premise servers with the instances in your VPC. Option B is incorrect as you normally create a VPN connection based off of a customer gateway and a virtual private gateway (VPG) in AWS. Option C is incorrect as EIPs are not needed as the instances in the VPC can communicate with on-premise servers via their private IP address. Option D is CORRECT because, there should not be a conflict between IP address of on-premise servers and the instances in VPC for them to communicate. Option E is incorrect because, Route53 is not useful in resolving on-premise dependency. Option F is CORRECT because VM Import Export service helps you to import the virtual machine images from the data center to AWS platform as EC2 instances and export them back to your on-premises environment. This offering allows you to leverage your existing investments in the virtual machines that you have built to meet your IT security, configuration management, and compliance requirements by bringing those virtual machines into Amazon EC2 as ready-to-use instances. The correct answers are: An AWS Direct Connect link between the VPC and the network housing the internal services., An IP address space that does not conflict with the one on-premises, A VM Import of the current virtual machine.
✓ A VM Import of the current virtual machine.

Q33)

An administrator has granted temporary credentials from STS to a set of users. It is later realized that these credentials should not have been given.

Can these credentials be revoked?

✓ Correct
Explanation:-For more information, please refer to the below link https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_revoke-sessions.html The correct answer is: True
● Incorrect

Q34)

Your company's on-premises content management system has the following architecture: Application Tier

– Java code on a JBoss application server Database Tier

– Oracle database regularly backed up to Amazon Simple Storage Service (S3) using the Oracle RMAN backup utility Static Content

– stored on a 512GB gateway stored Storage Gateway volume attached to the application server via the iSCSI interface

Which AWS based disaster recovery strategy will give you the best RTO?

● Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Restore the static content from an AWS Storage Gateway-VTL running on Amazon EC2
● Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Restore the static content by attaching an AWS Storage Gateway running on Amazon EC2 as an iSCSI volume to the JBoss EC2 server.
● Deploy the Oracle database on RDS. Deploy the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon Glacier. Generate an EBS volume of static content from the Storage Gateway and attach it to the JBoss EC2 server.
✓ Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Generate an EBS volume of static content from the Storage Gateway and attach it to the JBoss EC2 server.

Q35)

An application store a set of files in a single Amazon S3 bucket. Users will upload files from their mobile device directly to Amazon S3 and will be able to view and download their uploaded files directly from Amazon S3.

You want to configure security to handle potentially millions of users in the most secure manner possible.

What should your server-side application do when a new user registers on the mobile application?

● Create IAM user. Assign appropriate permissions to the IAM user Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
● Record the user's Information In Amazon DynamoDB. When the user uses their mobile app create temporary credentials using AWS Security Token Service with appropriate permissions, store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.
✓ Record the user's Information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app create temporary credentials using the AWS Security Token Service 'AssumeRole' function, store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.

Explanation:-This scenario requires the mobile application to have access to S3 bucket. There are potentially millions of users and a proper security measure should be taken. In such question, where mobile applications needs to access AWS Resources, always think about using funtions such as "AssumeRole", "AssumeRoleWithSAML", and "AssumeRoleWithWebIdentity". See the following diagram that explains the flow of actions while using "AssumeRole". You can let users sign in using a well-known third-party identity provider such as login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) 2.0 compatible provider. You can exchange the credentials from that provider for temporary permissions to use resources in your AWS account. This is known as the web identity federation approach to temporary access. When you use web identity federation for your mobile or web application, you don't need to create custom sign-in code or manage your own user identities. Using web identity federation helps you keep your AWS account secure because you don't have to distribute long-term security credentials, such as IAM user access keys, with your application. Option A is incorrect because you should always grant the short term or temporary credentials for the mobile application. This option asks to create a long term credentials. Option B is CORRECT because (a) it creates an IAM Role with appropriate permissions, (b) it generates temporary security credentials using STS "AssumeRole" function, and (c) it generates new credentials when the user runs the app the next time. Option C is incorrect because, even though the set up is very similar to option B, it does not create IAM Role with proper permissions which is an essential step. Option D is incorrect because, it asks to create an IAM User, not the IAM Role - which is not a good solution. You should create a IAM Role so that the app can access the AWS Resource via "AssumeRole" function. Option E is incorrect because, it asks to create an IAM User, not the IAM Role - which is not a good solution. You should create a IAM Role so that the app can access the AWS Resource via "AssumeRole" function. For more information on AWS temporary credentials, please refer to the below link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html The correct answer is: Record the user's Information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app create temporary credentials using the AWS Security Token Service 'AssumeRole' function, store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.

● Create a set of long-term credentials using AWS Security Token Service with appropriate permissions Store these credentials in the mobile app and use them to access Amazon S3.

Q36)

You currently have a placement group of instances. When you try to add new instances to the group, you receive a 'capacity error'.

Which of the following actions will most likely fix this problem? Choose the correct option from the below:

● Request a capacity increase from AWS as you are initially limited to 10 instances per Placement Group.
✓ Stop and restart the instances in the Placement Group and then try the launch again.
● Make a new Placement Group and launch the new instances in the new group. Make sure the Placement Groups are in the same subnet.
● Make sure all the instances are the same size and then try the launch again.

Q37) If you want to deliver private content to users from an S3 bucket, which of the below options is the most feasible to fulfill this requirement? Choose an option from the below:

● Use SQS to deliver content from the S3 bucket
● Use EC2 to deliver content from the S3 bucket
✓ Use pre-signed URL
● None of these

Q38) Explain what the following resource in a CloudFormation template does. Choose the best possible answer. SNSTopic : { "Type" : "AWS::SNS::Topic", "Properties" : { "Subscription" : [{ "Protocol" : "sqs", "Endpoint" : { "Fn::GetAtt" : ["SQSQueue", "Arn"] } }] }

● Creates an SNS topic and adds a subscription ARN endpoint for the SQS resource created under the logical name SQSQueue
✓ Creates an SNS topic and then invokes the call to create an SQS queue with a logical resource name of SQSQueue
● Creates an SNS topic and adds a subscription ARN endpoint for the SQS resource named Arn
● Creates an SNS topic which allows SQS subscription endpoints to be added as a parameter on the template

Q39)

An ERP application is deployed in multiple Availability Zones in a single region. In the event of failure, the RTO must be less than 3 hours and the RPO is 15 minutes. The customer realizes that data corruption occurred roughly 1.5 hours ago.

Which DR strategy can be used to achieve this RTO and RPO in the event of this kind of failure?

● Take hourly DB backups to an Amazon EC2 instance store volume, with transaction logs stored in Amazon S3 every 5 minutes.
✓ Take hourly DB backups to Amazon S3, with transaction logs stored in S3 every 5 minutes.
● Use synchronous database master-slave replication between two Availability Zones.
● Take 15-minute DB backups stored in Amazon Glacier, with transaction logs stored in Amazon S3 every 5 minutes.

Q40)

A user is trying to save some cost on the AWS services.

Which of the below-mentioned options will not help him to save cost?

● Delete the AWS ELB after all the instances behind it are terminated.
● Release the elastic IP if not required once the instance is terminated.
✓ Delete the AutoScaling launch configuration after the instances are terminated.
● Delete the unutilized EBS volumes once the instance is terminated.

Q41)

You are designing network connectivity for your fat client application. The application is designed for business travelers who

must be able to connect to it from their hotel rooms, cafes, public Wi-Fi hotspots, and elsewhere on the Internet.

While you do not want to publish the application on the Internet.

Which network design meets the above requirements while minimizing deployment and operational costs? Choose the correct answer from the options below

✓ Configure an SSL VPN solution in a public subnet of your VPC, then install and configure SSL VPN client software on all user computers. Create a private subnet in your VPC and place your application servers in it.
● Configure an IPsec VPN connection, and provide the users with the configuration details. Create a public subnet in your VPC, and place your application servers in it.
● Implement AWS Direct Connect, and create a private interface to your VPC. Create a public subnet and place your application servers in it.
● Implement Elastic Load Balancing with an SSL listener that terminates the back-end connection to the application.

Q42) When one creates an encrypted EBS volume and attach it to a supported instance type, which of the following data types are encrypted? Choose 3 options from the below:

✓ All snapshots created from the volume
Explanation:-Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted: (i) Data at rest inside the volume (ii) All data moving between the volume and the instance (iii) All snapshots created from the volume (iv) All volumes created from those snapshots Based on this, options A, B, and D are all CORRECT. Option B is incorrect since the data that is copied to S3 is not encrypted. For more information on this, please visit the link below: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html The correct answers are: Data at rest inside the volume, All data moving between the volume and the instance, All snapshots created from the volume
● All data copied from the EBS volume to S3
✓ All data moving between the volume and the instance
Explanation:-Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted: (i) Data at rest inside the volume (ii) All data moving between the volume and the instance (iii) All snapshots created from the volume (iv) All volumes created from those snapshots Based on this, options A, B, and D are all CORRECT. Option B is incorrect since the data that is copied to S3 is not encrypted. For more information on this, please visit the link below: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html The correct answers are: Data at rest inside the volume, All data moving between the volume and the instance, All snapshots created from the volume
✓ Data at rest inside the volume
Explanation:-Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted: (i) Data at rest inside the volume (ii) All data moving between the volume and the instance (iii) All snapshots created from the volume (iv) All volumes created from those snapshots Based on this, options A, B, and D are all CORRECT. Option B is incorrect since the data that is copied to S3 is not encrypted. For more information on this, please visit the link below: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html The correct answers are: Data at rest inside the volume, All data moving between the volume and the instance, All snapshots created from the volume

Q43)

You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets.

One instance is running a database and the other instance an application that will interface with the database.

You want to confirm that they can talk to each other for your application to work properly.

Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC? Choose 2 correct options from the below:

✓ Security groups are set to allow the application host to talk to the database on the right port/protocol
Explanation:-In order to have the instances communicate with each other, you need to properly configure both Security Group and Network access control lists (NACLs). For the exam, remember that Security Group operates at the instance level; where as, the NACL operates at subnet level. Option A is CORRECT because the security groups must be defined in order to allow web server to communicate with the database server. An example image from the AWS documentation is given below: Option B is incorrect because it is not necessary to have the two instances of the same type or be using same key-pair. Option C is incorrect because configuring NAT instance or NAT gateway will not enable the two servers to communicate with each other. NAT instance/NAT gateway are used to enable the communication between instances in the private subnets and internet. Option D is CORRECT because the two servers are in two separate subnets. In order for them to communicate with each other, you need to have the NACL's configured as shown below: For more information on VPC and Subnets, please visit the below URL: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html The correct answers are: A network ACL that allows communication between the two subnets, Security groups are set to allow the application host to talk to the database on the right port/protocol
● That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate
● Both instances are the same instance class and using the same Key-pair
✓ A network ACL that allows communication between the two subnets
Explanation:-In order to have the instances communicate with each other, you need to properly configure both Security Group and Network access control lists (NACLs). For the exam, remember that Security Group operates at the instance level; where as, the NACL operates at subnet level. Option A is CORRECT because the security groups must be defined in order to allow web server to communicate with the database server. An example image from the AWS documentation is given below: Option B is incorrect because it is not necessary to have the two instances of the same type or be using same key-pair. Option C is incorrect because configuring NAT instance or NAT gateway will not enable the two servers to communicate with each other. NAT instance/NAT gateway are used to enable the communication between instances in the private subnets and internet. Option D is CORRECT because the two servers are in two separate subnets. In order for them to communicate with each other, you need to have the NACL's configured as shown below: For more information on VPC and Subnets, please visit the below URL: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html The correct answers are: A network ACL that allows communication between the two subnets, Security groups are set to allow the application host to talk to the database on the right port/protocol

Q44)

A company has a requirement to host an application behind an AWS ELB.

The application will be supporting multiple device platforms.

Each device platform will need separate SSL certificates assigned to it.

Which of the below options is the best setup in AWS to fulfill the above requirement?

● Setup a hybrid architecture to handle multiple SSL certificates by using separate EC2 Instance groups running web applications for different platform types running in a VPC.

● Set up one ELB for all device platforms to distribute load among multiple instance under it. Each EC2 instance implements will have different SSL certificates assigned to it.

● You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disk, and decryption, when you access your objects.

✓ Create multiple ELB's for each type of certificate for each device platform.

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 SSL certificate setups are required for different platforms. The best approach is to create 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 will be very cumbersome and may not be feasible at all. Option C is incorrect because even though ELB supports multiple SSL certificates, distributing the load based on the platform type will not be feasible. You will still require multiple ELBs. 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 SSL termination logic. See the image below: For more information on ELB, please visit the below URL https://aws.amazon.com/elasticloadbalancing/classicloadbalancer/faqs/ The correct answer is: Create multiple ELB's for each type of certificate for each device platform.

Q45)

Server-side encryption is about data encryption at rest. That is, Amazon S3 encrypts your data at the object level as it writes it to disk in its data centers and decrypts it for you when you go to access it.

There are a few different options depending on how you choose to manage the encryption keys.

One of the options is called 'Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)'.

Which of the following best describes how this encryption method works? Choose the correct option from the below:

● You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disk, and decryption, when you access your objects.

● A randomly generated data encryption key is returned from Amazon S3, which is used by the client to encrypt the object data.

✓ Each object is encrypted with a unique key employing strong encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates.

Explanation:-Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. Option A is incorrect because there are no separate permissions to the key that protects the data key. Option B is CORRECT because as mentioned above, each object is encrypted with a strong unique key and that key itself is encypted by a master key. Option C is incorrect because the keys are managed by the AWS. Option D is incorrect because there is no randomly generated key and client does not do the encryption. For more information on S3 encryption, please visit the link https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html The correct answer is: Each object is encrypted with a unique key employing strong encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates.

● There are separate permissions for the use of an envelope key (that is, a key that protects your data's encryption key) that provides added protection against unauthorized access of your objects in S3 and also provides you with an audit trail of when your key was used and by whom.

Q46)

The Marketing Director in your company asked you to create a mobile app that lets users post sightings of good deeds known as random acts of kindness in 80-character summaries.

You decided to write the application in JavaScript so that it would run on the broadest range of phones, browsers, and tablets.

Your application should provide access to Amazon DynamoDB to store the good deed summaries. Initial testing of a prototype shows that there aren't large spikes in usage.

Which option provides the most cost-effective and scalable architecture for this application?

● Register the JavaScript application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow DynamoDB puts. You serve your mobile application out of Apache EC2 instances that are load-balanced and autoscaleYour EC2 instances are configured with an IAM role that allows DynamoDB puts. Your server updates DynamoDB

● Provide the JavaScript client with temporary credentials from the Security Token Service using a Token Vending Machine (TVM) to provide signed credentials mapped to an IAM user allowing DynamoDB puts. You serve your mobile application out of Apache EC2 instances that are load-balanced and autoscaled. Your EC2 instances are configured with an IAM role that allows DynamoDB puts. Your server updates DynamoDB.

✓ Register the application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow S3 gets and DynamoDB puts. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB.

Explanation:-This scenario asks to design a cost-effective and scalable solution where a multi-platform application needs to communicate with DynamoDB. For such scenarios, federated access to the application is the most likely solution. Option A is incorrect because the Token Vending Machine (STS Service) is implemented on a single EC2 instance which is a single point of failure. This is not a scalable solution either as the instance can become the performance bottleneck. Option B is CORRECT because, (i) it authenticates the application via federated identity provider such as Amazon, Google, Facebook etc, (ii) it sets up the proper permisssion for DynamoDB access, and (iii) S3 website which supports Javascript - is a highly scalable and cost effective solution. Option C is incorrect because deploying EC2 instances in auto-scaled environment is not as cost-effective solution as the S3 website, even though it is scalable. Option D is incorrect because (i) it does not mention any security token service that generates temporary credentials, and (ii) deploying EC2 instances in auto-scaled environment is not as cost-effective solution as the S3 website, even though it is scalable. The correct answer is: Register the application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow S3 gets and DynamoDB puts. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB.

● Provide the JavaScript client with temporary credentials from the Security Token Service using a Token Vending Machine (TVM) on an EC2 instance to provide signed credentials mapped to an Amazon Identity and Access Management (IAM) user allowing DynamoDB puts and S3 gets. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB.

Q47)

You currently have an EC2 instance with EBS volumes that store a lot of files.

It takes a long time for an application to process the files.

Which of the following options can be used to ensure the right storage option is used and to also ensure high availability of the application?

● EBS with Provisioned IOPS (PIOPS) to store I/O files. SNS to distribute elaboration commands to a group of hosts working in parallel Auto Scaling to dynamically size the group of hosts depending on the number of SNS notifications
● S3 to store I/O files, SNS to distribute evaporation commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the number of SNS notifications
● EBS with Provisioned IOPS (PIOPS) to store I/O files SQS to distribute elaboration commands to a group of hosts working in parallel. Use Auto Scaling to dynamically size the group of hosts depending on the length of the SQS queue
✓ S3 to store I/O files. SQS to distribute elaboration commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the length of the SQS queue
Explanation:-The scenario in this question is that (a) there any EC2 instances that need to process high number of input files, (b) currently the processing takes 20 hrs a day, which needs to be reduced, (c) the availability needs to be improved. Looking at all the option, it appears that there are two choices to be made. (1) between S3 and EBO with PIOPS, and (2) between SQS and SNS. First, let's see whether we should choose S3 or EBS with PIOPS. It appears that all the options have auto-scaling in common. i.e. there will be multiple EC2 instances working in parallel on the input data. This should reduce the overall elaboration time, satisfying one of the requirements. Since a single EBS volume cannot be attached to multiple instances, using EBS volume seems an illogical choice. Moreover, S3 provides high availability, which satisfies the other requirement. Second, SQS is a great option to do the autonomous tasks and can queue the service requests and can be scaled to meet the high demand. SNS is a mere notification service and would not hold the tasks. Hence, SQS is certainly the correct choice. Option A is CORRECT because, as mentioned above, it provides high availability, and can store the massive amount of data. Auto-scaling of EC2 instances reduces the overall processing time and SQS helps distributing the commands/tasks to the group of EC2 instances. Option B is incorrect because, as mentioned above, neither EBS nor SNS is a valid choice in this scenario. Option C is incorrect because, as mentioned above, SNS is not a valid choice in this scenario. Option D is incorrect because, as mentioned above, EBS is not a valid choice in this scenario. The correct answer is: S3 to store I/O files. SQS to distribute elaboration commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the length of the SQS queue

Q48)

An auditor has been called upon to carry out an audit of the configuration of your AWS accounts.

The auditor has specified that they just want to read only access to the AWS resources on all accounts.

Which of the below options would help the auditor get the required access?

● Create a custom identity broker application that allows the auditor to use existing Amazon credentials to log into the AWS environments.
● Configure an on-premise AD server and enable SAML and identify federation for single sign-on to each AWS account.
✓ Create an IAM role with read-only permissions to all AWS services in each AWS account. Create one auditor IAM account and add a permissions policy that allows the auditor to assume the ARN role for each AWS account that has an assigned role.
● Create an IAM user for each AWS account with read-only permission policies for the auditor, and disable each account when the audit is complete.

Q49) Which of the following are the recommendations from AWS when migrating a legacy application which is hosted on a virtual machine in an on-premise location? Choose 2 options from the below:

● Use entries in Amazon Route 53 that allow the Instance to resolve its dependencies' IP addresses on the on-premise location
✓ Use an Elastic IP address on the VPC instance
● Use a NAT instance to route traffic from the instance in the VPC.
✓ Use the VM Import facility provided by aws.

Q50)

A company currently has an on-premise location connecting to a VPC.

The company wants to have a dedicated network connection from the on-premise location to the VPC? Choose the correct answer from the below options which would help to fulfill the above requirement.

● Use a hardware VPN to connect both locations.
✓ Suggest provisioning a Direct Connect connection between the on-premise data center and the AWS region.
Explanation:-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: Suggest provisioning a Direct Connect connection between the on-premise data center and the AWS region.
● Provision a VPN connection between the on-premise data center and the AWS region using the VPN section of a VPC.
● Use a software VPN to connect both locations.