Answer Sheet

Q1)

An organization has configured Auto Scaling with ELB. There is a memory issue in the application which is causing CPU utilization to go above 90%.

The higher CPU usage triggers an event for Auto Scaling as per the scaling policy.

If the user wants to find the root cause inside the application without triggering a scaling activity, how can he achieve this?

- Stop the scaling process until research is completed.
- ✅ Suspend the scaling process until research is completed.

Explanation:-From the AWS documentation, it is very clear that the suspending process for Autoscaling can be used to debug root causes with the application.

- It is not possible to find the root cause from that instance without triggering scaling.
- Delete Auto Scaling until research is completed.

Q2)

A user has launched an EC2 instance store-backed instance in the US-East-1a zone.

The user created AMI #1 and copied it to the Europe region. After that, the user made a few updates to the application running in the US-East-1a zone.

The user makes an AMI#2 after the changes. If the user launches a new instance in Europe from the AMI #1 copy, which of the below-mentioned statements is true?

- The new instance will have the changes made after the AMI copy since AWS keeps updating the AMI.
- It is not possible to copy the instance store backed AMI from one region to another.
- The new instance will have the changes made after the AMI copy as AWS just copies the reference of the original AMI during the copying. Thus, the copied AMI will have all the updated data.
- ✅ The new instance in the EU region will not have the changes made after the AMI copy.

Explanation:-Every time you make a change to the instance you need to make an AMI out of it and copy it to the desired region. Only then will the instance created out of that AMI have the required changes.

Q3) Which of the following is an example of a good Amazon DynamoDB hash key schema for provisioned throughput efficiency? Choose an answer from the below options:

- Tuition Plan where the vast majority of students are in state and the rest are out of state.
- Class ID where every student is in one of the four classes.
- ✅ Student ID where every student has a unique ID.

Explanation:-Always have the primary key or hash key for those attributes which will have many values. And only option A fits that requirement. For more information on DynamoDB tables

- College ID where there are two colleges in the university.

Q4)

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 answers from the below options:

- ✅ Security groups are set to allow the application host to talk to the database on the right port/protocol.

Explanation:-When you design a web server and database server, the security groups must be defined so that the web server can talk to the database server. An example image from the AWS documentation is given below Also when communicating between subnets you need to have the NACL's defined Option B is wrong since the EC2 instances need not be the same class or same key pair to communicate to each other.

- Both instances are the same instance class and using the same Key-pair.
- That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate.
- ✅ A network ACL that allows communication between the two subnets.

Explanation:-When you design a web server and database server, the security groups must be defined so that the web server can talk to the database server. An example image from the AWS documentation is given below Also when communicating between subnets you need to have the NACL's defined Option B is wrong since the EC2 instances need not be the same class or same key pair to communicate to each other.

Q5) What is the feature Lambda@Edge used for in AWS? Choose an answer from the options given below:

- It is used specifically for the Edge based programing language.
- ✅ It is used for running Lambda functions at edge locations used by CloudFront.

Explanation:-Lambda@Edge allows you to run Lambda functions at the AWS edge locations in response to CloudFront events. Without Lambda@Edge, customized processing requires requests to be forwarded back to compute resources at the centralized servers. This slows down the user experience. Lambda@Edge supports Node.js, which is a server-side JavaScript framework. For more information on Lambda@Edge

- It can support any type of programming language.
- It is used for running Lambda functions at edge locations defined by S3.

Q6) While managing your instances in the current Opswork stack, you suddenly started getting the following error:

ws::CharlieInstanceService::Errors::UnrecognizedClientException - The security token included in the request is invalid. Which of the below 2 check can be done to rectify this error?

- Check if the Opswork client is configured properly.
- ✅ Check the IAM role which was attached to the instance.

Explanation:-This can occur if a resource outside AWS OpsWorks on which the instance depends was edited or deleted. The following are examples of resource changes that can break communications with an instance. An IAM user or role associated with the instance has been deleted accidentally, outside of AWS OpsWorks Stacks. This causes a communication failure between the AWS OpsWorks agent that is installed on the instance and the AWS OpsWorks Stacks service. The IAM user that is associated with an instance is required throughout the life of the instance. Editing volume or storage configurations while an instance is offline can make an instance unmanageable. Adding EC2 instances to an EIP manually. AWS OpsWorks reconfigures an assigned Elastic Load Balancing load balancer each time an instance enters or leaves the online state. AWS OpsWorks only considers instances it knows about to be valid members; instances that are added outside of AWS OpsWorks, or by some other process, are removed. Every other instance is removed.

- Check if the stack is configured properly.
- ✅ Check if the EIP have been added to the EC2 instances manually.

Explanation:-This can occur if a resource outside AWS OpsWorks on which the instance depends was edited or deleted. The following are examples of resource changes that can break communications with an instance. An IAM user or role associated with the instance has been deleted accidentally, outside of AWS OpsWorks Stacks. This causes a communication failure between the AWS OpsWorks agent that is installed on the instance and the AWS OpsWorks Stacks service. The IAM user that is associated with an instance is required throughout the life of the instance. Editing volume or storage configurations while an instance is offline can make an instance unmanageable. Adding EC2 instances to an EIP manually. AWS OpsWorks reconfigures an assigned Elastic Load Balancing load balancer each time an instance enters or leaves the online state. AWS OpsWorks only considers instances it knows about to be valid members; instances that are added outside of AWS OpsWorks, or by some other process, are removed. Every other instance is removed.

Q7)

A company has 2 accounts- one is a development account and the other is the production account. There are 20 people on the development account who now need various levels of access provided to them on the production account.

10 of them need read-only access to all resources on the production account, 5 of them need read/write access to EC2 resources, and the remaining 5 only need read-only access to S3 buckets.

Which of the following options would be the best way for both practically and security-wise to accomplish this task? Choose the correct answer from the below options:

- Create 3 new users on the production account with the various levels of permissions needed. Give each of the 20 users the login for whichever one of the 3 accounts they need depending on the level of access required.
- ✅ Create 3 roles in the production account with a different policy for each of the access levels needed. Add permissions to each IAM user on the developer account.

Explanation:-For access to any AWS service or for any type of security access, the ideal approach is to use roles. So one just needs to create the 3 roles in the production account and provide the relevant access.

- Copy the 20 users IAM accounts from the development account to the production account. Then change the access levels for each user on the production account.
- Create encryption keys for each of the resources that need access and provide those keys to each user depending on the access required.

Q8)

A large enterprise wants to adopt Cloud Formation to automate administrative tasks and implement the security principles of least privilege and separation of duties. They have identified the following roles with the corresponding tasks in the company: Network administrators: create, modify and delete VPCs, subnets, NACLs, routing tables and security groups.

Application operators: deploy complete application stacks (ELB, Auto-Scaling groups, RDS) whereas all resources must be deployed in the VPCs managed by the network administrators.

Both groups must maintain their own Cloud Formation templates and should be able to create, update and delete only their own Cloud Formation stacks.

The company has followed your advice to create two IAM groups, one for applications and one for networks.

Both IAM groups are attached to IAM policies that grant rights to perform the necessary task of each group as well as the creation, update, and deletion of Cloud Formation stacks.

Given setup and requirements, which statements represent valid design considerations? Choose 2 options from the below:

- ✅ Restricting the launch of EC2 instances into VPCs requires resource level permissions in the IAM policy of the application group.

Explanation:-explicitly launch instances, we need IAM permissions.

- Nesting network stacks within application stacks simplifies management and debugging, but requires resource level permissions in the IAM policy of the network group.
- The application stack cannot be deleted before all network stacks are deleted.
- Unless resource level permissions are used on the cloud formation: Delete Stack action, network administrators could tear down application stacks.
- ✅ Network stack updates will fail upon attempts to delete a subnet with EC2 instances.

Explanation:-subnets cannot be deleted with instances in them.

Q9) Which of the following media servers can be used for live media streaming with CloudFront? Choose 3 options from the below:

- Atlassian Media Servers
- ✅ Wowza streaming engine

Explanation:-The documentation on live streaming is given in the AWS CloudFront section.

- ✅ Adobe Media Server

Explanation:-The documentation on live streaming is given in the AWS CloudFront section.

- ✅ IIS Media services

Explanation:-The documentation on live streaming is given in the AWS CloudFront section.

Q10)

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

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

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

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

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

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

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

Explanation:-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.

- Create an RDS Read Replica for the batch analysis and SQS to send a message to the on-premises system to update the dashboard.

Q11) How can you ensure the scalability of the application developed in Java interfacing with DynamoDB to reduce the load on the DynamoDB database? Choose an answer from the below options:

- Increase write capacity of Dynamo DB to meet the peak loads.
- Launch DynamoDB in Multi-AZ configuration with a global index to balance writes.
- Add more DynamoDB databases to handle the load.
- ✅ Use SQS to assist and let the application pull messages and then perform the relevant operation in DynamoDB.

Explanation:-When the idea comes to scalability then SQS is the best option. Normally DynamoDB is scalable, but since one is looking for a cost-effective solution, the messaging in SQS can assist in managing the situation mentioned in the question. Amazon Simple Queue Service (SQS) is a fully-managed message queuing service for reliably communicating among distributed software components and microservices - at any scale. Building applications from individual components that each perform a discrete function improve scalability and reliability and is best practice design for modern applications. SQS makes it simple and cost-effective to decouple and coordinate the components of a cloud application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available For more information on SQS,

---

Q12) Which of the following types of servers would this CloudFormation template be most appropriate for? Choose a correct answer from the below options: { "AWSTemplateFormatVersion" : "2010-09-09", "Description" : "My CloudFormation Template", "Resources" : { "MyInstance" : { "Type" : "AWS::EC2::Instance", "Properties" : { "InstanceType" : "t2.micro", "ImageId" : "ami-030f4133", "NetworkInterfaces" : [{ "AssociatePublicIpAddress" : "true", "DeviceIndex" : "0", "DeleteOnTermination" : "true", "SubnetId" : "subnet-0c2c0855", "GroupSet" : ["sg-53a4e434"] }] } } } }

- Domain Controller
- ✅ Bastion host

Explanation:-The bastion host needs a minimum configuration and a public IP address. The above CloudFormation template best fits this.

- Database server
- Log collection server

Q13)

There is a requirement by a company that if an object is changed in their CloudFront deployment by the users in origin, it should reflect instantaneously in CloudFront.

How can you achieve this?

- Dynamic content cannot be served from the cloudfront
- Set TTL to 10 seconds
- ✅ Set TTL to 0 seconds

Explanation:-In CloudFront, to enforce the delivery of content to the user as soon as it gets changed by the origin, the time to live (TTL) should be set to 0. setting TTL to 0 will enforce the delivery of content to the user as soon as it gets changed by the origin.

- You have to contact AWS support center to enable this feature
- Use fast invalidate feature provided in cloudfront

Q14)

A recent increase in a number of users of an application hosted on an EC2 instance that you manage has caused the instance's OS to run out of CPU resources and crash.

The crash caused several users' unsaved data to be lost and your supervisor wants to know how this problem can be avoided in the future.

Which of the following would you not recommend? Choose the correct answer from the below options:

- ✅ Take frequent snapshots of the EBS volume during business hours to ensure users' data is backed up.

Explanation:-If you take snapshots during business hours, the situation can become worse since I/O is required to create the snapshot.

- Snapshot the EBS volume and re-deploy the application server as a larger instance type.

- Use autoscaling to deploy additional application server instances when load is high.
- Redesign the application so that users' unsaved data is periodically written to disk.

Q15) An organization (Account ID 121212). has attached the below-mentioned IAM policy to a user. What does this policy statement entitle the user to perform? { "Version": "2012-10-17", "Statement": [{ "Sid": "AllowUsersAllActionsForCredentials", "Effect": "Allow", "Action": ["iam:*LoginProfile", "iam:*AccessKey*", "iam:*SigningCertificate*"], "Resource": ["arn:aws:iam::121212:user/${aws:username}"] }] }

- The policy allows the IAM user to modify all credentials using only the console.
- ✅ The policy allows the user to modify all IAM user's password, sign in certificates and access keys using only CLI, SDK or APIs.

Explanation:-First, in order to give a user a certain set of policies, you need to mention the following line. The aws:username will apply to the AWS logged in user. Resource": "arn:aws:iam::account-id-without-hyphens:user/${aws:username} Nex,t the policies will give the permissions to modify all IAM user's password, sign in certificates and access keys using only CLI, SDK or APIs "iam:*LoginProfile", "iam:*AccessKey*", "iam:*SigningCertificate*"

- The policy allows the IAM user to modify all IAM user's credentials using the console, SDK, CLI or APIs.
- The policy will give an invalid resource error.

Q16)

There is a requirement for a high availability and disaster recovery plan for an organization. Below are the key points for this plan Data cannot be lost, this is the key requirement.

Recovery time can be long as this could save on cost

Which of the following options would be the best one for this corporation, given the concerns that they have outlined to you above? Choose the correct answer from the below options:

- ✅ Backup and restoring with S3 should be considered due to the low cost of S3 storage. Backup up frequently and the data can be sent to S3 using either Direct Connect or Storage Gateway, or over the Internet.

Explanation:-Amazon S3 is storage for the Internet. It's a simple storage service that offers software developers a highly-scalable, reliable, and low-latency data storage infrastructure at very low costs.

- Set up pre-configured servers using Amazon Machine Images. Use an Elastic IP and Route 53 to quickly switch over to your new infrastructure if there are any problems when you run your health checks.
- Make sure you have RDS set up as an asynchronous Multi-AZ deployment, which automatically provisions and maintains an asynchronous "standby" replica in a different Availability Zone.
- Set up a number of smaller instances in a different region, which all have Auto Scaling and Elastic Load Balancing enabled. If there is a network outage, then these instances will auto scale up. As long as spot instances are used and the instances are small this should remain a cost effective solution.

Q17) A company needs to monitor the read and write IOPs metrics for their AWS MySQL RDS instance and send real-time alerts to their operations team. Which AWS services can accomplish this? Choose 2 options from the below:

- Amazon Simple Email Service
- ✅ Amazon CloudWatch

Explanation:-CloudWatch is used for monitoring the metrics pertaining to the AWS resources.

- ✅ Amazon Simple Notification Service

Explanation:-SNS is used for sending the real time notifications based on the thresholds set in CloudWatch.

- Amazon Route 53
- Amazon Simple Queue Service

Q18) How can you secure data at rest on an EBS volume?

- Write the data randomly instead of sequentially.
- Attach the volume to an instance using EC2's SSL interface.
- ✅ Use an encrypted file system on top of the EBS volume.

Explanation:-In order to secure data at rest on an EBS volume, you either have to encrypt the volume when it is being created or encrypt the data after the volume is created.

- Encrypt the volume using the S3 server-side encryption service.
- Create an IAM policy that restricts read and write access to the volume.

Q19)

A public archives organization is about to move a pilot application they are running on AWS into production. You have been hired to analyze their application architecture and give cost-saving recommendations.

The application displays scanned historical documents.

Each document is split into individual image tiles at multiple zoom levels to improve responsiveness and ease of use for the end users.

At maximum zoom level the average document will be 8000 X 6000 pixels in size, split into multiple 40px X 40px image tiles.

The tiles are batch processed by Amazon Elastic Compute Cloud (EC2) instances and put into an Amazon Simple Storage Service (S3) bucket.

A browser-based JavaScript viewer fetches tiles from the Amazon (S3) bucket and displays them to users as they zoom and pan around each document.

The average storage size of all zoom levels for a document is approximately 30MB of JPEG tiles.

Originals of each document are archived in Amazon Glacier.

The company expects to process and host over 500,000 scanned documents in the first year.

What are your recommendations? Choose 3 options from the below:

- Decrease the size (width/height) of the individual tiles at the maximum zoom level.
- ✓ Use Amazon S3 Reduced Redundancy Storage for each zoom level.

Explanation:-RRS is a low cost storage option and will help keeping the overall cost low.

- ✓ Increase the size (width/height) of the individual tiles at the maximum zoom level.

Explanation:-increasing the size of the images would help reduce the cost of number of GET/PUT requests on the origin server.

- ✓ Deploy an Amazon CloudFront distribution in front of the Amazon S3 tiles bucket.

Explanation:-the caching is done by CloudFront via the edge locations which reduces the load on the origin.

- Store the maximum zoom level in the low cost Amazon S3 Glacier option and only retrieve the most frequently access tiles as they are requested by users.

Q20)

A user is using a small MySQL RDS DB. The user is experiencing high latency due to the Multi-AZ feature.

Which of the below-mentioned options may not help the user in this situation?

- Schedule the automated back up in non-working hours
- ✓ Take a snapshot from standby Replica

Explanation:-In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups As per AWS, the below are the best practices for multiAZ. For production workloads, we recommend you use Provisioned IOPS and DB instance classes (m1.large and larger) that are optimized for Provisioned IOPS for fast, consistent performance.

- Use IOPS
- Use a large or higher size instance

Q21)

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

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

- The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.
- 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:-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.

- Create a role that has the required permissions for the auditor.

Q22)

A client is using CloudFront with a source which normally serves dynamic content. There is a requirement that as soon the content is changed in the source, it is delivered to the client.

Which of the following configuration can be made to fulfill this requirement?

- ✓ Set TTL to 0 seconds

Explanation:-You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. The low TTL is also given in the AWS documentation.

- Set TTL to 10 seconds
- You have to contact AWS support center to enable this feature
- Dynamic content cannot be served from the cloudfront
- Use fast invalidate feature provided in cloudfront

Q23)

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user's data center.

The user's data center has CIDR 172.28.0.0/12.

The user has also setup a NAT instance (i-123456) to allow traffic to the internet from the VPN subnet.

Which of the below-mentioned options is not a valid entry for the main route table in this scenario?

- Destination: 20.0.0.0/16 and Target: local
- ✓ Destination: 20.0.1.0/24 and Target: i-12345

Explanation:-The below diagram shows how a typical setup for a VPC with VPN and Internet gateway would look like. The only routing option which should have access to the internet gateway should be the 0.0.0.0/0 address.

- Destination: 172.28.0.0/12 and Target: vgw-12345
- Destination: 0.0.0.0/0 and Target: i-12345

Q24)

A company has setup a DirectConnect connection between their on-premise location and their AWS VPC.

They want to setup redundancy in case the DirectConnect connection fails.

What can they do in this regard? Choose 2 options from the below:

✅ Setup an IPSec VPN Connection

Explanation:-This is clearly mentioned in the AWS FAQs. If you have established a second AWS Direct Connect connection, traffic will failover to the second link automatically. We recommend enabling Bidirectional Forwarding Detection (BFD) when configuring your connections to ensure fast detection and failover. If you have configured a backup IPsec VPN connection instead, all VPC traffic will failover to the VPN connection automatically. Traffic to/from public resources such as Amazon S3 will be routed over the Internet. If you do not have a backup AWS Direct Connect link or an IPsec VPN link, then Amazon VPC traffic will be dropped in the event of a failure. Traffic to/from public resources will be routed over the Internet.

✅ Setup another DirectConnect connection

Explanation:-This is clearly mentioned in the AWS FAQs. If you have established a second AWS Direct Connect connection, traffic will failover to the second link automatically. We recommend enabling Bidirectional Forwarding Detection (BFD) when configuring your connections to ensure fast detection and failover. If you have configured a backup IPsec VPN connection instead, all VPC traffic will failover to the VPN connection automatically. Traffic to/from public resources such as Amazon S3 will be routed over the Internet. If you do not have a backup AWS Direct Connect link or an IPsec VPN link, then Amazon VPC traffic will be dropped in the event of a failure. Traffic to/from public resources will be routed over the Internet.

- Setup a connection via EC2 instances
- Setup S3 connection

Q25)

A user has created a public subnet with VPC and launched an EC2 instance within it. The user is trying to delete the subnet.

What will happen in this scenario?

- It will delete the subnet and make the EC2 instance as a part of the default subnet.
- The subnet can never be deleted independently, but the user has to delete the VPC first.

✅ It will not allow the user to delete the subnet until the instances are terminated.

Explanation:-In AWS, when you try to delete a subnet which has instances it will not allow to delete it. The below error message will be shown when u try to delete a subnet with instances.

- It will delete the subnet as well as terminate the instances.

Q26) Which of the following are correct statements with policy evaluation logic in AWS Identity and Access Management? Choose 2 answers from the below options:

- An explicit allow overrides an explicit deny

✅ By default, all requests are denied

Explanation:-As per the evaluation logic, it is clear that the above scenario leads to a default deny.

- By default, all request are allowed

✅ An explicit allow overrides default deny

Explanation:-As per the evaluation logic, it is clear that the above scenario leads to a default deny.

- An explicit deny does not override an explicit allow

Q27) What are the 2 types of snapshots that are supported by AWS Redshift? Choose 2 answers from the options given below:

✅ Automated

Explanation:-Snapshots are point-in-time backups of a cluster. There are two types of snapshots: automated and manual. Amazon Redshift stores these snapshots internally in Amazon S3 by using an encrypted Secure Sockets Layer (SSL) connection. If you need to restore from a snapshot, Amazon Redshift creates a new cluster and imports data from the snapshot that you specify.

✅ Manual

Explanation:-Snapshots are point-in-time backups of a cluster. There are two types of snapshots: automated and manual. Amazon Redshift stores these snapshots internally in Amazon S3 by using an encrypted Secure Sockets Layer (SSL) connection. If you need to restore from a snapshot, Amazon Redshift creates a new cluster and imports data from the snapshot that you specify.

- Primary
- Default

Q28)

A company is in the evaluation phase of deploying a redshift cluster.

Which of the following types of instances should the company think of deploying for their redshift cluster during this phase? Choose an answer from the options given below:

- Combination of all 3 types of instances
- Reserved instances because they are cost effective

✅ On-Demand

Explanation:-In the evaluation phase of your project or when you're developing a proof of concept, on-demand pricing gives you the flexibility to pay as you go, to pay only for what you use, and to stop paying at any time by shutting down or deleting clusters. After you have established the needs of your production environment and begin the implementation phase, you should consider reserving compute nodes by purchasing one or more offerings.

- Spot Instances because they are the least cost option

Q29) Which of the following are best practices that need to be followed when updating Opswork stack instances with the latest security patches? Choose 2 correct options from the below:

Delete the entire stack and create a new one.

Create and start new instances to replace your current online instances.

Explanation:-As per the AWS documentation, below are the best practices for updating your Opswork stacks instances with the latest security patches. Create and start new instances to replace your current online instances. Then delete the current instances. The new instances will have the latest set of security patches installed during setup. On Linux-based instances in Chef 11.10 or older stacks, run the Update Dependencies stack command, which installs the current set of security patches and other updates on the specified instances.

Use Cloudformation to deploy the security patches.

run the Update Dependencies stack command for Linux based instances.

Explanation:-As per the AWS documentation, below are the best practices for updating your Opswork stacks instances with the latest security patches. Create and start new instances to replace your current online instances. Then delete the current instances. The new instances will have the latest set of security patches installed during setup. On Linux-based instances in Chef 11.10 or older stacks, run the Update Dependencies stack command, which installs the current set of security patches and other updates on the specified instances.

Q30) Which of the below-mentioned ways can be used to provide additional layers of protection to all your EC2 resources? Choose the correct answer from the below options:

Ensure that the proper tagging strategies have been implemented to identify all of your EC2 resources.

Add policies which have deny and/or allow permissions on tagged resources.

Add an IP address condition to policies that specify that requests to EC2 instances should come from a specific IP address or CIDR block range.

All actions listed here would provide additional layers of protection.

Q31) Which of the following options will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket? Choose 3 options from the below:

Configuring IAM role

Explanation:-In questions like this where an application, or user needs to be given access using Single Sign On (SSO), following steps are very important: (i) setting up a identity provider for federated access (ii) authenticating users using corporate data store / active directory-user-attributes/ (iii) getting temporary access tokens / credentials using AWS STS (iv) creating the IAM Role that has the access to the needed AWS Resources. as mentioned above, creating the IAM Role that has the access to the needed AWS Resources is needed.

Setting up a federation proxy or identity provider

Explanation:-In questions like this where an application, or user needs to be given access using Single Sign On (SSO), following steps are very important: (i) setting up a identity provider for federated access (ii) authenticating users using corporate data store / active directory-user-attributes/ (iii) getting temporary access tokens / credentials using AWS STS (iv) creating the IAM Role that has the access to the needed AWS Resources. as mentioned above, setting up a identity provider for federated access is needed.

Tagging each folder in the bucket

Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket

Using AWS Security Token Service to generate temporary tokens

Explanation:-In questions like this where an application, or user needs to be given access using Single Sign On (SSO), following steps are very important: (i) setting up a identity provider for federated access (ii) authenticating users using corporate data store / active directory-user-attributes/ (iii) getting temporary access tokens / credentials using AWS STS (iv) creating the IAM Role that has the access to the needed AWS Resources. as mentioned above, getting temporary access tokens / credentials using AWS STS is needed.

Q32)

A user is planning to set up-the Multi-AZ feature of RDS.

Which of the below-mentioned conditions won't take advantage of the Multi-AZ feature?

A manual failover of the DB instance using Reboot with failover option

Region outage

Explanation:-As per the aws documentation all the failover conditions are given and Region Outage will not make use of multi AZ.

Availability zone outage

When the user changes the DB instance's server type

Q33) Which of the following can be used as an origin server in CloudFront? Choose 3 answers from the options given below:

A webserver running in your own datacenter

Explanation:-Currently, Cloudfront supports the following types of distributions S3 buckets - When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. Custom Origin - A custom origin is an HTTP server, for example, a web server. The HTTP server can be an Amazon EC2 instance or an HTTP server that you manage privately. When you use a custom origin, you specify the DNS name of the server, along with the HTTP and HTTPS ports and the protocol that you want CloudFront to use when fetching objects from your origin.

An Amazon S3 bucket

Explanation:-Currently, Cloudfront supports the following types of distributions S3 buckets - When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. Custom Origin - A custom origin is an HTTP server, for example, a web server. The HTTP server can be an Amazon EC2 instance or an HTTP server that you manage privately. When you use a custom origin, you specify the DNS name of the server, along with the HTTP and HTTPS ports and the protocol that you want CloudFront to use when fetching objects from your origin.

A webserver running on EC2

Explanation:-Currently, Cloudfront supports the following types of distributions S3 buckets - When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. Custom Origin - A custom origin is an HTTP server, for example, a web server. The HTTP server can be an Amazon EC2 instance or an HTTP server that you manage privately. When you use a custom origin, you specify the DNS name of the server, along with the HTTP and HTTPS ports and the protocol that you want CloudFront to use when fetching objects from your origin.

A RDS instance

Q34) Your team is excited about the use of AWS because now they have access to "programmable Infrastructure". You have

been asked to manage your AWS infrastructure In a manner similar to the way you might manage application code You want to be able to deploy exact copies of different versions of your infrastructure, stage changes into different environments, revert back to previous versions, and identify what versions are running at any particular time (development test QA . production). Which approach addresses this requirement?

- Use cost allocation reports and AWS Opsworks to deploy and manage your infrastructure.
- Use AWS CloudWatch metrics and alerts along with resource tagging to deploy and manage your infrastructure.
- Use AWS Beanstalk and a version control system like GIT to deploy and manage your infrastructure.
- ✅ Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructure.

Explanation:-AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. You can use AWS Cloud Formation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You don't need to figure out the order for provisioning AWS services or the subtleties of making those dependencies work. CloudFormation takes care of this for you. After the AWS resources are deployed, you can modify and update them in a controlled and predictable way, in effect applying version control to your AWS infrastructure the same way you do with your software. You can also visualize your templates as diagrams and edit them using a drag-and-drop interface with the AWS CloudFormation Designer. Option A is incorrect because Cost Allocation Reports is not helpful for the purpose of the question. Option B is incorrect because Cloudwatch is used for monitoring. Option C is incorrect because it does have the concept of programmable Infrastructure.

Q35)

A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16.

The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24.

The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306).

The user is configuring a security group of the NAT instance.

Which of the below-mentioned entries is not required for the NAT security group?

- For Outbound allow Destination: 0.0.0.0/0 on port 443
- ✅ For Inbound allow Source: 20.0.0.0/24 on port 80

Explanation:-As per AWS, below are the recommended rules for a NAT instance. Hence based on the best practice, Option C is not the right option.

- For Outbound allow Destination: 0.0.0.0/0 on port 80
- For Inbound allow Source: 20.0.1.0/24 on port 80

Q36)

A mobile application needs access to a DynamoDB table.

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 below options:

- ✅ 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:-For access to any AWS service, the ideal approach for any application is to use Roles. This is the first preference.

- 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 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 assumed with AssumeRoleWithSAML.
- During the install and game configuration process, have each user create an IAM credential and assign the IAM user to a group with proper permissions to communicate with DynamoDB.

Q37)

A company has developed a sensor intended to be placed inside of people's watches, monitoring the number of steps taken every day.

There is an expectation of thousands of sensors reporting in every minute and hopes to scale to millions by the end of the year.

A requirement for the project is it needs to be able to accept the data, run it through ETL to store in warehouse and archive it on Amazon Glacier, with room for a real-time dashboard for the sensor data to be added at a later date.

What is the best method for architecting this application given the requirements? Choose the correct answer from the below options:

- Write the sensor data directly to a saleable DynamoDB; create a data pipeline that starts an EMR cluster using data from DynamoDB and sends the data to S3 and Redshift.
- ✅ Write the sensor data directly to Amazon Kinesis and output the data into Amazon S3 creating a lifecycle policy for Glacier archiving. Also, have a parallel processing application that runs the data through EMR and sends to a Redshift data warehouse.

Explanation:-Since part of the question is archival to Glacier, it means the starting point ideally can be S3.

- Write the sensor data to Amazon S3 with a lifecycle policy for Glacier, create an EMR cluster that uses the bucket data and runs it through ETL. It then outputs that data into Redshift data warehouse.
- Use Amazon Cognito to accept the data when the user pairs the sensor to the phone, and then have Cognito send the data to Dynamodb. Use Data Pipeline to create a job that takes the DynamoDB table and sends it to an EMR cluster for ETL, then outputs to Redshift and S3 while, using S3 lifecycle policies to archive on Glacier.

Q38) Which of the following HTTP methods are supported by Amazon CloudFront? Choose 3 options from the below

- ✅ POST

Explanation:-Amazon CloudFront supports the following HTTP methods: GET, HEAD, POST, PUT, DELETE, OPTIONS, and PATCH. This means

you can improve the performance of dynamic websites that have web forms, comment, and login boxes, “add to cart” buttons or other features that upload data from end users.

- UPDATE
- ✅ GET

Explanation:-Amazon CloudFront supports the following HTTP methods: GET, HEAD, POST, PUT, DELETE, OPTIONS, and PATCH. This means you can improve the performance of dynamic websites that have web forms, comment, and login boxes, “add to cart” buttons or other features that upload data from end users.

- ✅ DELETE

Explanation:-Amazon CloudFront supports the following HTTP methods: GET, HEAD, POST, PUT, DELETE, OPTIONS, and PATCH. This means you can improve the performance of dynamic websites that have web forms, comment, and login boxes, “add to cart” buttons or other features that upload data from end users.

Q39) What can be done in Cloudfront to ensure that as soon as the content is changed in the source, it is delivered to the client? Choose an answer from the options below options.

- Set TTL to 10 seconds
- ✅ Set TTL to 0 seconds

Explanation:-In CloudFront, to enforce the delivery of content to the user as soon as it gets changed by the origin, the time to live (TTL) should be set to 0. setting TTL to 0 will enforce the delivery of content to the user as soon as it gets changed by the origin.

- Dynamic content cannot be served from the cloudfront
- Use fast invalidate feature provided in cloudfront
- You have to contact AWS support center to enable this feature

---

Q40)

You've been working on a CloudFront whole site CDN. After configuring the whole site CDN with a custom CNAME and supported HTTPS custom domain (i.e., https://domain.com) you open domain.com and are receiving the following error “CloudFront wasn't able to connect to the origin.”

What might be the most likely cause of this error and how would you fix it? Choose the correct answer from the below options:

- The HTTPS certificate is expired or missing a third party signer. To resolve this purchase and add a new SSL certificate.
- The origin on the CloudFront distribution is the wrong origin.
- ✅ The Origin Protocol Policy is set to Match Viewer and HTTPS isn't configured on the origin.

Explanation:-It is clearly given in the AWS documentation that the Origin Protocol Policy should be set accordingly.

- TCP HTTPS isn't configured on the CloudFront distribution but is configured on the CloudFront origin.

Q41) Which AWS Feature can allow secure communication between multiple sites each with their own customer gateway? Choose an answer from the options given below:

- VPC
- ✅ VPN CloudHub

Explanation:-If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. This enables your remote sites to communicate with each other, and not just with the VPC. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who'd like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.

- VPN Cloud
- Virtual private gateway

Q42)

As an IT administrator, you have been requested to manage the CloudFormation stacks for a set of developers in your company.

A set of web and database developers will be working on the application.

How would you design the CloudFormation stacks in the best way possible?

- Create one stack for the web and database developers.
- ✅ Create separate stacks for the web and database developers.

Explanation:-The following use case scenario is given in the AWS documentation to support the answer: For example, imagine a team of developers and engineers who own a website that is hosted on autoscaling instances behind a load balancer. Because the website has its own lifecycle and is maintained by the website team, you can create a stack for the website and its resources. Now imagine that the website also uses back-end databases, where the databases are in a separate stack that is owned and maintained by database administrators. Whenever the website team or database team needs to update their resources, they can do so without affecting each other's stack. If all resources were in a single stack, coordinating and communicating updates can be difficult.

- CloudFormation is not the right fit, use Opswork instead.
- Define separate EC2 instances since defining Cloudformation can get cumbersome.

Q43)

A user has created a mobile application which makes calls to DynamoDB to fetch certain data.

The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile.

Which of the below-mentioned statements is true with respect to the best practice for security in this scenario?

- The user should create a separate IAM user for each mobile application and provide DynamoDB access with it.
- ✅ The application should use an IAM role with web identity federation which validates calls to DynamoDB with identity providers, such as Google, Amazon, and Facebook.

Explanation:-With web identity federation, you don't need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) —such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account And always the best way to authenticate is to ensure that you create an IAM role which can then be assigned to the EC2 instance.

- The user should create an IAM role with DynamoDB and EC2 access. Attach the role with EC2 and route all calls from the mobile through EC2.
- Create an IAM Role with DynamoDB access and attach it with the mobile application.

Q44)

You have created an Opsworks stack to create EC2 instances along with an ELB.

You have now been asked to change the region in which the EC2 instances will be registered.

Can you change the region value in the Opswork stack?

- Correct
- ✅ Incorrect

Explanation:-After you create a layer, some properties (such as AWS region) are immutable, but you can change most of the layer configuration at any time.

Q45)

A customer is hosting their company website on a cluster of web servers that are behind a public-facing load balancer.

The customer also uses Amazon Route 53 to manage their public DNS.

How should the customer configure the DNS zone apex record to point to the load balancer?

- Create a CNAME record pointing to the load balancer DNS name.
- Create an A record pointing to the IP address of the load balancer.
- Create a CNAME record aliased to the load balancer DNS name.
- ✅ Create an A record aliased to the load balancer DNS name.

Explanation:-Alias resource record sets are virtual records that work like CNAME records. But they differ from CNAME records in that they are not visible to resolvers. Resolvers only see the A record and the resulting IP address of the target record. As such, unlike CNAME records, alias resource record sets are available to configure a zone apex (also known as a root domain or naked domain) in a dynamic environment.

Q46)

You are moving an existing traditional system to AWS. During migration, you discover that the master server is the single point of failure.

Having examined the implementation of the master server you realize that there is not enough time during migration to re-engineer it to be highly available.

You also discover that it stores its state in local MySQL database.

In order to minimize downtime, you select RDS to replace the local database and configure the master to use it.

What steps would best allow you to create a self-healing architecture?

- Replicate the local database into a RDS Read Replica. Place the master node into a multi-AZ auto-scaling group with a minimum of one and maximum of one with health checks.
- Replicate the local database into a RDS Read Replica. Place the master node into a Cross Zone ELB with a minimum of one and maximum of one with health checks.
- Migrate the local database into Multi-AZ database. Place the master node into a Cross Zone ELB with a minimum of one and maximum of one with health checks.
- ✅ Migrate the local database into Multi-AZ database. Place the master node into a multi-AZ auto-scaling group with a minimum of one and maximum of one with health checks.

Explanation:-Multi-AZ is used for highly available architecture. If a failover happens, the secondary DB which is a synchronous replica will have the data, and it's just the CNAME which changes. For Read replica, it's primarily used for distributing workloads.

Q47)

Your company policies require encryption of sensitive data at rest.

You are considering the possible options for protecting data while storing it at rest on an EBS data volume, attached to an EC2 instance.

Which of these options would allow you to encrypt your data at rest? Choose 3 options from the below

- ✅ Encrypt data using native data encryption drivers at the file system level

Explanation:-You can encrypt the data at rest by either using a native data encryption, using a third party encrypting tool, or just encrypt the data before storing on the volume. it uses the native data encryption.

- Implement SSL/TLS for all services running on the server
- ✅ Encrypt data inside your applications before storing it on EBS

Explanation:-You can encrypt the data at rest by either using a native data encryption, using a third party encrypting tool, or just encrypt the data before storing on the volume. it encypts the data before storing it on EBS.

- Do nothing as EBS volumes are encrypted by default
- ✅ Implement third party volume encryption tools

Explanation:-You can encrypt the data at rest by either using a native data encryption, using a third party encrypting tool, or just encrypt the data before storing on the volume. it uses third party volume encryption tool.

Q48)

As an IT administrator, you have been tasked to ensure that SQL injection attacks are kept at bay.

You currently maintain a set of applications hosted on AWS which consists of a fleet of EC2 instances.

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

- 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.
- Create NACL rules for the subnet hosting the application.
- ✓ 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:-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.

- Create a DirectConnect connection so that your have a dedicated connection line.

Q49)

Which of the following items are required to allow an application deployed on an EC2 instance to write data to a DynamoDB table.

Assume that no security keys are allowed to be stored on the EC2 instance. Choose 3 options from the below:

- ✓ Create an IAM Role that allows write access to the DynamoDB table

Explanation:-To enable an AWS service to access another one, the most important requirement is to create an appropriate IAM Role and attaching that role to the service that needs the access. it create the appropriate IAM Role for accessing the DynamoDB table.

- Create an IAM User that allows write access to the DynamoDB table
- ✓ Launch an EC2 Instance with the IAM Role included in the launch configuration

Explanation:-To enable an AWS service to access another one, the most important requirement is to create an appropriate IAM Role and attaching that role to the service that needs the access. it launches the EC2 instance after attaching the required role.

- ✓ Add an IAM Role to a running EC2 instance

Explanation:-To enable an AWS service to access another one, the most important requirement is to create an appropriate IAM Role and attaching that role to the service that needs the access. you can attach the role to a running EC2 instance that needs the access.

- Add an IAM User to a running EC2 instance

Q50)

Your fortune 500 company has undertaken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware. The outcome was that all employees would be granted access to use Amazon S3 for storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket? Choose 3 options from the below

- ✓ Using AWS Security Token Service to generate temporary tokens

Explanation:-In questions like this where an application, or user needs to be given access using Single Sign On (SSO), following steps are very important: (i) setting up a identity provider for federated access (ii) authenticating users using corporate data store / active directory-user-attributes/ (iii) getting temporary access tokens / credentials using AWS STS (iv) creating the IAM Role that has the access to the needed AWS Resources. getting temporary access tokens / credentials using AWS STS is needed.

- ✓ Setting up a federation proxy or identity provider

Explanation:-In questions like this where an application, or user needs to be given access using Single Sign On (SSO), following steps are very important: (i) setting up a identity provider for federated access (ii) authenticating users using corporate data store / active directory-user-attributes/ (iii) getting temporary access tokens / credentials using AWS STS (iv) creating the IAM Role that has the access to the needed AWS Resources. setting up a identity provider for federated access is needed.

- Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket
- Tagging each folder in the bucket
- ✓ Configuring IAM role

Explanation:-In questions like this where an application, or user needs to be given access using Single Sign On (SSO), following steps are very important: (i) setting up a identity provider for federated access (ii) authenticating users using corporate data store / active directory-user-attributes/ (iii) getting temporary access tokens / credentials using AWS STS (iv) creating the IAM Role that has the access to the needed AWS Resources. creating the IAM Role that has the access to the needed AWS Resources is needed.
