Answer Sheet

Q1)

A user has granted read/write permission of his S3 bucket using ACL.

Which of the below mentioned options is a valid ID to grant permission to other AWS accounts (grantee) using ACL?

- S3 Secure ID
- ✅ Canonical user ID

Explanation:-An S3 bucket ACL grantee can be an AWS account or one of the predefined Amazon S3 groups. The user can grant permission to an AWS account by the email address of that account or by the canonical user ID. If the user provides an email in the grant request, Amazon S3 finds the canonical user ID for that account and adds it to the ACL. The resulting ACL will always contain the canonical user ID for the AWS account, and not the AWS account's email address.

- IAM User ID
- Access ID

Q2)

A user has launched an EC2 Windows instance from an instance store backed AMI. The user wants to convert the AMI to an EBS backed AMI.

How can the user convert it?

- Attach an EBS volume to the instance and unbundle all the AMI bundled data inside the EBS
- Attach an EBS volume and use the copy command to copy all the ephermal content to the EBS volume
- ✅ A Windows based instance store backed AMI cannot be converted to an EBS backed AMI

Explanation:-Generally when a user has launched an EC2 instance from an instance store backed AMI, it can be converted to an EBS backed AMI provided the user has attached the EBS volume to the instance and unbundles the AMI data to it. However, if the instance is a Windows instance, AWS does not allow this. In this case, since the instance is a Windows instance, the user cannot convert it to an EBS backed AMI.

- It is not possible to convert an instance store backed AMI to an EBS backed AMI

Q3)

A user is running a batch process on EBS backed EC2 instances. The batch process starts a few instances to process hadoop Map reduce jobs which can run between 50 – 600 minutes or sometimes for more time.

The user wants to configure that the instance gets terminated only when the process is completed.

How can the user configure this with CloudWatch?

- It is not possible to terminate instances automatically
- Setup the CloudWatch with Auto Scaling to terminate all the instances
- Setup a job which terminates all instances after 600 minutes
- ✅ Setup the CloudWatch action to terminate the instance when the CPU utilization is less than 5%

Explanation:-Amazon CloudWatch alarm watches a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which terminates the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action.

Q4)

A user has recently started using EC2. The user launched one EC2 instance in the default subnet in EC2-VPC.

Which of the below mentioned options is not attached or available with the EC2 instance when it is launched?

- Internet gateway
- Public IP address
- ✅ Elastic IP

Explanation:-A Virtual Private Cloud (VPC) is a virtual network dedicated to a user's AWS account. A subnet is a range of IP addresses in the VPC. The user can launch the AWS resources into a subnet. There are two supported platforms into which a user can launch instances: EC2-Classic and EC2-VPC (default subnet). A default VPC has all the benefits of EC2-VPC and the ease of use of EC2-Classic. Each instance that the user launches into a default subnet has a private IP address and a public IP address. These instances can communicate with the internet through an internet gateway. An internet gateway enables the EC2 instances to connect to the internet through the Amazon EC2 network edge.

- Private IP address

Q5)

A user is trying to delete an Auto Scaling group from CLI.

Which of the below mentioned steps are to be performed by the user?

- Terminate the Auto Scaling instances with the as-terminate-instance command
- There is no need to change the capacity. Run the as-delete-group command and it will reset all values to 0
- ✅ Set the minimum size and desired capacity to 0

Explanation:-If the user wants to delete the Auto Scaling group, the user should manually set the values of the minimum and desired capacity to 0. Otherwise Auto Scaling will not allow for the deletion of the group from CLI. While trying from the AWS console, the user need not set the values to 0 as the Auto Scaling console will automatically do so.

- Terminate the instances with the ec2-terminate-instance command

Q6)

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

The public subnet uses CIDR 20.0.1.0/24.

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 for the public subnet (WebSecGrp) and the private subnet (DBSecGrp).

Which of the below mentioned entries is required in the private subnet database security group (DBSecGrp)?

- Allow Inbound on port 3306 from source 20.0.0.0/16
- Allow Outbound on port 80 for Destination NAT Instance IP
- ✅ Allow Inbound on port 3306 for Source Web Server Security Group (WebSecGrp)

Explanation:-A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet to host the web server and DB server respectively, the user should configure that the instances in the private subnet can receive inbound traffic from the public subnet on the DB port. Thus, configure port 3306 in Inbound with the source as the Web Server Security Group (WebSecGrp). The user should configure ports 80 and 443 for Destination 0.0.0.0/0 as the route table directs traffic to the NAT instance from the private subnet.

- Allow Outbound on port 3306 for Destination Web Server Security Group (WebSecGrp)

Q7)

A user has launched an EC2 instance from an instance store backed AMI.

If the user restarts the instance, what will happen to the ephermal storage data?

- ✅ The data is preserved

Explanation:-A user can reboot an EC2 instance using the AWS console, the Amazon EC2 CLI or the Amazon EC2 API. Rebooting an instance is equivalent to rebooting an operating system. However, it is recommended that the user use Amazon EC2 to reboot the instance instead of running the operating system reboot command from the instance. When an instance launched from an instance store backed AMI is rebooted all the ephermal storage data is still preserved.

- All the data will be erased but the ephermal storage will stay connected
- All data will be erased and the ephermal storage is released
- It is not possible to restart an instance launched from an instance store backed AMI

Q8)

A user is trying to connect to a running EC2 instance using SSH. However, the user gets an Unprotected Private Key File error.

Which of the below mentioned options can be a possible reason for rejection?

- The user has provided the wrong user name for the OS login
- ✅ The private key file has the wrong file permission

Explanation:-While doing SSH to an EC2 instance, if you get an Unprotected Private Key File error it means that the private key file's permissions on your computer are too open. Ideally the private key should have the Unix permission of 0400. To fix that, run the command:
chmod 0400 /path/to/private.key

- The public key file has the wrong permission
- The ppk file used for SSH is read only

Q9) An orgnization has applied the below mentioned policy on an IAM group which has selected the IAM users. What entitlements do the IAM users avail with this policy?

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
]
}
```

- If this policy is applied to the EC2 resource, the users of the group will have full access to the EC2 resources
- The policy is not created correctly. It will throw an error for wrong resource name
- ✅ It allows full access to all AWS services for the IAM users who are a part of this group

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. The IAM group allows the organization to specify permissions for a collection of users. With the below mentioned policy, it will allow the group full access (Admin) to all AWS services.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
]
}
```

- The policy is for the group. Thus, the IAM user cannot have any entitlement to this

---

Q10) An organization (account ID 123412341234) has configured the IAM policy to allow the user to modify his credentials. What will the below mentioned statement allow the user to perform?

```
{
“Version”: “2012-10-17”,
“Statement”: [{
“Effect”: “Allow”,
“Action”: [
“iam:AddUserToGroup”,
“iam:RemoveUserFromGroup”,
“iam:GetGroup”
],
“Resource”: “arn:aws:iam:: 123412341234:group/TestingGroup”
}]
```

- Allow the IAM user to delete the TestingGroup
- ✅ Allow the IAM user to update the membership of the group called TestingGroup

Explanation:-AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the organization (account ID 123412341234) wants their users to manage their subscription to the groups, they should create a relevant policy for that. The below mentioned policy allows the respective IAM user to update the membership of the group called MarketingGroup.

```
{
“Version”: “2012-10-17”,
“Statement”: [{
“Effect”: “Allow”,
“Action”: [
“iam:AddUserToGroup”,
“iam:RemoveUserFromGroup”,
“iam:GetGroup”
],
“Resource”: “arn:aws:iam:: 123412341234:group/ TestingGroup ”
}]
```

- The IAM policy will allow the user to subscribe to any IAM group
- The IAM policy will throw an error due to an invalid resource name

---

Q11)

A user has launched an EBS backed instance with EC2-Classic. The user stops and starts the instance.

Which of the below mentioned statements is not true with respect to the stop/start action?

- ✅ The Elastic IP remains associated with the instance

Explanation:-A user can always stop/start an EBS backed EC2 instance. When the user stops the instance, it first enters the stopping state, and then the stopped state. AWS does not charge the running cost but charges only for the EBS storage cost. If the instance is running in EC2-Classic, it receives a new private IP address; as the Elastic IP address (EIP) associated with the instance is no longer associated with that instance.

- The instance may run on a anew host computer
- The volume is preserved
- The instance gets new private and public IP addresses

Q12)

A user has created a launch configuration for Auto Scaling where CloudWatch detailed monitoring is disabled. The user wants to now enable detailed monitoring.

How can the user achieve this?

- The user should change the Auto Scaling group from the AWS console to enable detailed monitoring
- Update the Launch config with CLI to set InstanceMonitoring.Enabled = true
- ✅ Create a new Launch Config with detail monitoring enabled and update the Auto Scaling group
- Update the Launch config with CLI to set InstanceMonitoringDisabled = false

---

Q13)

A user is planning to setup infrastructure on AWS for the Christmas sales. The user is planning to use Auto Scaling based on the schedule for proactive scaling.

What advise would you give to the user?

- ✅ Wait till end of November before scheduling the activity

Explanation:-Auto Scaling based on a schedule allows the user to scale the application in response to predictable load changes. The user can specify any date in the future to scale up or down during that period. As per Auto Scaling the user can schedule an action for up to a month in the future. Thus, it is recommended to wait until end of November before scheduling for Christmas.

- It is good to schedule now because if the user forgets later on it will not scale up
- It is not advisable to use scheduled based scaling
- The scaling should be setup only one week before Christmas

Q14)

A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25. The user is trying to create the private subnet with CIDR 20.0.0.128/25.

Which of the below mentioned statements is true in this scenario?

- It will not allow the user to create the private subnet due to a CIDR overlap
- ✓ It will allow the user to create a private subnet with CIDR as 20.0.0.128/25
- This statement is wrong as AWS does not allow CIDR 20.0.0.0/25

Explanation:-When the user creates a subnet in VPC, he specifies the CIDR block for the subnet. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset (to enable multiple subnets). If the user creates more than one subnet in a VPC, the CIDR blocks of the subnets must not overlap. Thus, in this case the user has created a VPC with the CIDR block 20.0.0.0/24, which supports 256 IP addresses (20.0.0.0 to 20.0.0.255). The user can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses the CIDR block 20.0.0.0/25 (for addresses 20.0.0.0 – 20.0.0.127) and the other uses the CIDR block 20.0.0.128/25 (for addresses 20.0.0.128 – 20.0.0.255).

- It will not allow the user to create a private subnet due to a wrong CIDR range

---

Q15)

A user has created an ELB with three instances.

How many security groups will ELB create by default?

- 3

Explanation:-Elastic Load Balancing provides a special Amazon EC2 source security group that the user can use to ensure that back-end EC2 instances receive traffic only from Elastic Load Balancing. This feature needs two security groups: the source security group and a security group that defines the ingress rules for the back-end instances. To ensure that traffic only flows between the load balancer and the back-end instances, the user can add or modify a rule to the back-end security group which can limit the ingress traffic. Thus, it can come only from the source security group provided by Elastic load Balancing.

- 5
- ✓ 2
- 1

Q16)

A user has configured an EC2 instance in the US-East-1a zone. The user has enabled detailed monitoring of the instance.

The user is trying to get the data from CloudWatch using a CLI.

Which of the below mentioned CloudWatch endpoint URLs should the user use?

- monitoring.us-east-1-a.amazonaws.com
- ✓ monitoring.us-east-1.amazonaws.com

Explanation:-The CloudWatch resources are always region specific and they will have the end point as region specific. If the user is trying to access the metric in the US-East-1 region, the endpoint URL will be: monitoring.us-east-1.amazonaws.com

- monitoring.us-east-1a.amazonaws.com
- cloudwatch.us-east-1a.amazonaws.com

Q17)

A user has configured ELB with two EBS backed EC2 instances. The user is trying to understand the DNS access and IP support for ELB.

Which of the below mentioned statements may not help the user understand the IP mechanism supported by ELB?

- The client can connect over IPV4 or IPV6 using Dualstack
- Communication between the load balancer and back-end instances is always through IPV4
- ELB DNS supports both IPV4 and IPV6
- ✓ The ELB supports either IPV4 or IPV6 but not both

Explanation:-Elastic Load Balancing supports both Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4). Clients can connect to the user's load balancer using either IPv4 or IPv6 (in EC2-Classic) DNS. However, communication between the load balancer and its back-end instances uses only IPv4. The user can use the Dualstack-prefixed DNS name to enable IPv6 support for communications between the client and the load balancers. Thus, the clients are able to access the load balancer using either IPv4 or IPv6 as their individual connectivity needs dictate.

Q18)

A user has created an ELB with the availability zone US-East-1A. The user wants to add more zones to ELB to achieve High Availability.

How can the user add more zones to the existing ELB?

- The user should stop the ELB and add zones and instances as required
- The only option is to launch instances in different zones and add to ELB
- It is not possible to add more zones to the existing ELB
- ✓ The user can add zones on the fly from the AWS console

Q19)

A user is trying to connect to a running EC2 instance using SSH. However, the user gets a Host key not found error.

Which of the below mentioned options is a possible reason for rejection?

- The instance CPU is heavily loaded
- The access key to connect to the instance is wrong
- ✓ The user has provided the wrong user name for the OS login

Explanation:-If the user is trying to connect to a Linux EC2 instance and receives the Host Key not found error the probable reasons are:

The private key pair is not right
The user name to login is wrong
- The security group is not configured properly

Q20)

A user has setup an RDS DB with Oracle. The user wants to get notifications when someone modifies the security group of that DB.

How can the user configure that?

- It is not possible to get the notifications on a change in the security group
- Configure the CloudWatch alarm on the DB for a change in the security group
- Configure SNS to monitor security group changes
- ✅ Configure event notification on the DB security group

Q21)

A user has setup connection draining with ELB to allow in-flight requests to continue while the instance is being deregistered through Auto Scaling.

If the user has not specified the draining time, how long will ELB allow in-flight requests traffic to continue?

- 0 seconds
- 3600 seconds
- ✅ 300 seconds
- 600 seconds

Q22)

A user has moved an object to Glacier using the life cycle rules. The user requests to restore the archive after 6 months. When the restore request is completed the user accesses that archive.

Which of the below mentioned statements is not true in this condition?

- The user can modify the restoration period only by issuing a new restore request with the updated period
- The user needs to pay storage for both RRS (restored) and Glacier (Archive) rates
- ✅ The restored object's storage class will be RRS

Explanation:-AWS Glacier is an archival service offered by AWS. AWS S3 provides lifecycle rules to archive and restore objects from S3 to Glacier. Once the object is archived their storage class will change to Glacier. If the user sends a request for restore, the storage class will still be Glacier for the restored object. The user will be paying for both the archived copy as well as for the restored object. The object is available only for the duration specified in the restore request and if the user wants to modify that period, he has to raise another restore request with the updated duration.

- The archive will be available as an object for the duration specified by the user during the restoration request

---

Q23)

A user has created a queue named "awsmodule" with SQS. One of the consumers of queue is down for 3 days and then becomes available.

Will that component receive message from queue?

- No, since SQS sends message to consumers who are available that time
- Yes, since SQS will not delete message until it is delivered to all consumers
- No, since SQS by default stores message for 1 day only
- ✅ Yes, since SQS by default stores message for 4 days

Q24)

A user is trying to create a PIOPS EBS volume with 3 GB size and 90 IOPS.

Will AWS create the volume?

- Yes, since PIOPS is higher than 100
- No, since the PIOPS and EBS size ratio is less than 30
- ✅ No, the EBS size is less than 4GB

Explanation:-A Provisioned IOPS (SSD) volume can range in size from 4 GiB to 16 TiB and you can provision up to 20,000 IOPS per volume.

- Yes, since the ratio between EBS and IOPS is less than 30

Q25) A user has created an ELB with Auto Scaling. Which of the below mentioned offerings from ELB helps the user to stop sending new requests traffic from the load balancer to the EC2 instance when the instance is being deregistered while continuing in-flight requests?

- ELB auto registration Off
- ✅ ELB connection draining

Explanation:-The Elastic Load Balancer connection draining feature causes the load balancer to stop sending new requests to the back-end instances when the instances are deregistering or become unhealthy, while ensuring that in-flight requests continue to be served.

- ELB deregistration check
- ELB sticky session

Q26)

A user has stored data on an encrypted EBS volume. The user wants to share the data with his friend's AWS account.

How can user achieve this?

- If both the accounts are using the same encryption key then the user can share the volume directly
- Take a snapshot and share the snapshot with a friend
- ✅ Copy the data to an unencrypted volume and then share

Explanation:-AWS EBS supports encryption of the volume. It also supports creating volumes from existing snapshots provided the snapshots are created from encrypted volumes. If the user is having data on an encrypted volume and is trying to share it with others, he has to copy the data from the encrypted volume to a new unencrypted volume. Only then can the user share it as an encrypted volume data. Otherwise the snapshot cannot be shared.

- Create an AMI from the volume and share the AMI

Q27)

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?

- When the user changes the DB instance's server type
- ✅ Region outage

Explanation:-Amazon RDS when enabled with Multi AZ will handle failovers automatically. Thus, the user can resume database operations as quickly as possible without administrative intervention. The primary DB instance switches over automatically to the standby replica if any of the following conditions occur:
An Availability Zone outage
The primary DB instance fails
The DB instance's server type is changed
The DB instance is undergoing software patching
A manual failover of the DB instance was initiated using Reboot with failover

- Availability zone outage
- A manual failover of the DB instance using Reboot with failover option

---

Q28)

A system admin is managing buckets, objects and folders with AWS S3.

Which of the below mentioned statements is true and should be taken in consideration by the sysadmin?

- Both the object and bucket can have an Access Policy but folder cannot have policy
- ✅ The folders support only ACL

Explanation:-A sysadmin can grant permission to the S3 objects or the buckets to any user or make objects public using the bucket policy and user policy. Both use the JSON-based access policy language. Generally if user is defining the ACL on the bucket, the objects in the bucket do not inherit it and vice a versa. The bucket policy can be defined at the bucket level which allows the objects as well as the bucket to be public with a single policy applied to that bucket. It cannot be applied at the object level. The folders are similar to objects with no content. Thus, folders can have only ACL and cannot have a policy.

- Both the object and bucket can have ACL but folders cannot have ACL
- Folders can have a policy

Q29)

A user has launched an EC2 instance. However, due to some reason the instance was terminated.

If the user wants to find out the reason for termination, where can he find the details?

- The user can get information from the AWS console, by checking the Instance description under the Instance Status Change reason label
- It is not possible to find the details after the instance is terminated
- The user can get information from the AWS console, by checking the Instance description under the Instance Termination reason label
- ✅ The user can get information from the AWS console, by checking the Instance description under the State transition reason label

Explanation:-An EC2 instance, once terminated, may be available in the AWS console for a while after termination. The user can find the details about the termination from the description tab under the label State transition reason. If the instance is still running, there will be no reason listed. If the user has explicitly stopped or terminated the instance, the reason will be "User initiated shutdown".

Q30)

A root account owner has given full access of his S3 bucket to one of the IAM users using the bucket ACL.

When the IAM user logs in to the S3 console, which actions can he perform?

- He can just view the content of the bucket
- The IAM user can perform all operations on the bucket using only API/SDK
- He can do all the operations on the bucket
- ✅ It is not possible to give access to an IAM user using ACL

Explanation:-Each AWS S3 bucket and object has an ACL (Access Control List) associated with it. An ACL is a list of grants identifying the grantee and the permission granted. The user can use ACLs to grant basic read/write permissions to other AWS accounts. ACLs use an Amazon S3–specific XML schema. The user cannot grant permissions to other users (IAM users) in his account.

Q31)

A user has launched an EC2 instance and deployed a production application in it.

The user wants to prohibit any mistakes from the production team to avoid accidental termination.

How can the user achieve this?

✅ The user can the set DisableApiTermination attribute to avoid accidental termination

Explanation:-It is always possible that someone can terminate an EC2 instance using the Amazon EC2 console, command line interface or API by mistake. If the admin wants to prevent the instance from being accidentally terminated, he can enable termination protection for that instance. The DisableApiTermination attribute controls whether the instance can be terminated using the console, CLI or API. By default, termination protection is disabled for an EC2 instance. When it is set it will not allow the user to terminate the instance from CLI, API or the console.

- The user can set the Deletion termination flag to avoid accidental termination
- The user can set the InstanceInitiatedShutdownBehavior flag to avoid accidental termination
- It is not possible to avoid accidental termination

Q32)

An organization has added 3 of his AWS accounts to consolidated billing. One of the AWS accounts has purchased a Reserved Instance (RI) of a small instance size in the US-East-1a zone.

All other AWS accounts are running instances of a small size in the same zone.

What will happen in this case for the RI pricing?

- If there are more than one instances of a small size running across multiple accounts in the same zone no one will get the benefit of RI

✅ Any single instance from all the three accounts can get the benefit of AWS RI pricing if they are running in the same zone and are of the same size

Explanation:-AWS consolidated billing enables the organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. For billing purposes, consolidated billing treats all the accounts on the consolidated bill as one account. This means that all accounts on a consolidated bill can receive the hourly cost benefit of the Amazon EC2 Reserved Instances purchased by any other account. In this case only one Reserved Instance has been purchased by one account. Thus, only a single instance from any of the accounts will get the advantage of RI. AWS will implement the blended rate for each instance if more than one instance is running concurrently.

- One instance of a small size and running in the US-East-1a zone of each AWS account will get the benefit of RI pricing
- Only the account that has purchased the RI will get the advantage of RI pricing

---

Q33)

A user wants to capture errors that occur in the AWS MySQL RDS DB.

Which of the below mentioned activities may help the user to get the data easily?

- It is not possible to get the log files for MySQL RDS

✅ Direct the error log to a DB table and then query that table

Explanation:-The user can view, download, and watch the database logs using the Amazon RDS console, the Command Line Interface (CLI) or the Amazon RDS API. For the MySQL RDS, the user can view the error log, slow query log, and general logs. The user can also view the MySQL logs easily by directing the logs to a database table in the main database and querying that table.

- Find all the transaction logs and query on those records
- Download the log file to DynamoDB and search for records

Q34) How would you restore an EBS snapshot to an EC2 instance? Choose the correct answer:

✅ Create a new volume from the snapshot, attach the volume to the EC2 instance, pre-warm the volume and mount it to the device

Explanation:-Create a new volume from the snapshot, attach the volume to the EC2 instance, pre-warm the volume and mount it to the device

- Clone the snapshot
- Mount the device, create a volume from the snapshot, and mount the volume
- Attach the volume to the EC2 instance, create a snapshot and clone the data

---

Q35)

You are running a legacy application that has a hard coded IP address in your application.

How might you apply high availability to the instance running that application? Choose the correct answer:

- Re-hard code the IP address in your application

✅ Assign an elastic IP address to the EC2 instance, have a backup instance running. In the event of failure, move Elastic IP from the primary instance to the backup instance.

Explanation:-Assign an elastic IP address to the EC2 instance, have a backup instance running. In the event of failure, move Elastic IP from the primary instance to the backup instance

- None of these
- You can't do this .

Q36) What item, when attached to a subnet, will allow the internal subnet to communicate to external networks? Choose the 2 correct answers:

✅ IGW Internet Gateway

✅ Virtual Private Gateway

- Customer Gateway
- NAT instance

Q37)

You see an increased load on an EC2 instance that is used as a web server. You decide placing the server behind an Elastic Load Balancer and deploying an additional instance should help meet this increased demand on system resources.

You deploy the ELB, configure it to listen for traffic on port 80, bring up a second EC2 instance, move both instances behind the load balancer, and provide customers with the ELB's URL – https://mywebapp-1234567890.us-west-2.elb.amazonaws.com.

You immediately begin receiving complaints that customers cannot connect to the web application via the ELB's URL.

Why? Choose the correct answer:

- You specified https:// in the ELB's URL, but the EC2 instances are not configured to listen on port 443
- You specified https:// in the ELB's URL, but the EC2 instances are not configured to listen on port 80.
- The ELB's URL is not publicly accessible. You need to create an Alias record in Route 53 for the ELB.
- ✅ You specified https:// in the ELB's URL, but the ELB is not configured to listen on port 443.

Explanation:-Specifying https:// directs web traffic to port 443. If you only configured a listener for port 80 on the ELB, traffic on port 443 will not be accepted.

Q38)

Your Infrastructure does not have an Internet gateway attached to any of the subnets.

What might you do in order to SSH into your EC2 instances?

All other configuration is correct. Choose the correct answer:

- Open up port 22 on your security groups
- Open up port 22 on your subnets
- Bastion host
- ✅ Create a VPN connection

Q39) What might be the cause of an EC2 instance not launching in an auto-scaling group? Choose the 3 correct answers:

- ✅ Key pair associated with EC2 instance does not exist

Explanation:-Availability zone is no longer supported, Invalid EBS device mapping, Key pair associated with EC2 instance does not exist

- Security group placement
- ✅ Invalid EBS device mapping

Explanation:-Availability zone is no longer supported, Invalid EBS device mapping, Key pair associated with EC2 instance does not exist

- ✅ Availability zone is no longer supported

Explanation:-Availability zone is no longer supported, Invalid EBS device mapping, Key pair associated with EC2 instance does not exist

---

Q40) If we want to be able to monitor billing and cost metrics, what AWS services do we need to enable and use together? Choose the correct answer

- CloudWatch
- ✅ Account Preferences Billing Alerts
- CloudFormation
- CloudFront

Q41)

In your LAMP application, you have some developers that say they would like access to your logs.

However, since you are using an AWS Auto Scaling group, your instances are constantly being re-created.

What would you do to make sure that these developers can access these log files? Choose the correct answer:

- Give only the necessary access to the Apache servers so that the developers can gain access to the log files.
- ✅ Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Explanation:-Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access

- Give read-only access to your developers to the Apache servers.
- Give root access to your Apache servers to the developers.

Q42)

You run a stateless web application with the following components: an Elastic Load Balancer, three Web/Application servers on EC2, and a MySQL RDS database with 5000 Provisioned IOPS.

Average response time for users is increasing.

Looking at CloudWatch, you observe 95% CPU usage on the Web/Application servers and 20% CPU usage on the database.

The average number of database disk operations varies between 2000 and 2500.

How would you improve performance? (Choose Two) Choose the 2 correct answers:

- Use Scaling to add additional Web/Application servers based on a memory usage threshold
- ✅ Choose a different EC2 instance type for the Web/Application servers with a more appropriate CPU/Memory ratio

Explanation:-Choose a different EC2 instance type for the Web/Application servers with a more appropriate CPU/Memory ratio, Use Auto Scaling to add additional Web/Application servers based on CPU load threshold

- ✅ Use Auto Scaling to add additional Web/Application servers based on CPU load threshold

Explanation:-Choose a different EC2 instance type for the Web/Application servers with a more appropriate CPU/Memory ratio, Use Auto Scaling to add additional Web/Application servers based on CPU load threshold

- Increase the number of open TCP connections allowed per web/application EC2 instance

---

Q43)

Your applications in AWS need to authenticate against LDAP credentials that are in your on-premises data center. You need low latency between the AWS app authenticating between AWS and your on- premises network.

How can you achieve this? Choose the correct answer:

- You don't have to use LDAP to authenticate to your apps.
- ✅ If you don't already have a secure tunnel, create a VPN between your on-premises data center and AWS. Once you have a VPN tunnel established between the data centers then you can spin up a secondary LDAP server that replicates from on premises LDAP server.

Explanation:-If you don't already have a secure tunnel, create a VPN between your on-premises data center and AWS. Once you have a VPN tunnel established between the data centers then you can spin up a secondary LDAP server that replicates from on premises LDAP server

- Create a new LDAP server and authenticate to it.
- Create a Direct Connect tunnel and you can authenticate faster.

Q44)

You have been tasked with identifying an appropriate storage solution for a NoSQL database that requires random I/O reads of greater than 10,000 4kB IOPS.

Which EC2 option will meet this requirement? Choose the correct answer:

- High Storage instance configured in RAID 10
- ✅ EBS optimized instances

Explanation:-EBS volumes only allow you to provision up to 4,000k IOPS per volume. EBS optimized instances have greater IOPs and can go up to 16K

- SSD instance store
- EBS provisioned IOPS

Q45)

You have enabled a CloudWatch metric on your Redis ElastiCache cluster. Your alarm is triggered due to an increased amount of evictions.

How might you go about solving the increased eviction errors from the ElastiCache cluster? Choose the correct answer:

- Reboot your node
- If you exceed your chosen threshold, scale your cache cluster out and add read replicas
- Add a node to the cluster
- ✅ Increase the size of your node

Q46)

You have decided to extend your on-site data center to Amazon Web Servers by creating a VPC. You already have multiple DNS servers on the premises.

You are using these DNS servers to host DNS records for your internal applications.

You have a corporate security network policy that says that a DNS name for an internal application can only be resolved internally and never publicly over the internet.

Your existing on-premises data center is already connected to your VPC using IPSec VPN.

You are deploying new applications within your AWS service that need to resolve these new applications by name.

How might you set up the scalable DNS architecture? Choose the correct answer:

- Created a new Route 53 hosted zone and forward your internal DNS queries out to the internet.
- Using Route 53 hosted zones, you can use all internal domain names' A record sets.
- Create secondary DNS servers on a Linux server and replicate from primary DNS servers on your on-premises
- ✅ Create a DNS option set that includes both the DHCP options with domain-name-servers=AmazonProvidedDNS and your internal DNS servers

Explanation:-Create a DNS option set that includes both the DHCP options with domain-name-servers=AmazonProvidedDNS and your internal DNS servers

---

Q47)

You manage EC2 instances in two different VPCs and you would like instances in both VPCs to be able to easily communicate with each other. You are considering using VPC peering.

Will this work? (Choose Two) Choose the 2 correct answers:

- ✅ Yes, as long as the VPCs' CIDR blocks don't overlap.

Explanation:-Yes, as long as the VPC's are in the same region., Yes, as long as the VPCs' CIDR blocks don't overlap.

- Yes, as long as the VPCs are in the same account.
- Yes, as long as all EC2 instances have a public IP.
- ✅ Yes, as long as the VPC's are in the same region.

Explanation:-Yes, as long as the VPC's are in the same region., Yes, as long as the VPCs' CIDR blocks don't overlap.

Q48)

You notice that several of your AWS environment's CloudWatch metrics are hovering near a value of 100.

Which of these are you least concerned about? Choose the correct answer:

- RDS CPU Utilization
- ✅ ElastiCache CurrConnections

Explanation:-A high number of connections is not necessarily a bad thing, if there are adequate resources to service those connections. 100% usage of resources, as in options A and C, typically means they are strained under a heavy load. A high SpilloverCount for an Elastic Load Balancer is also bad, as you do not want requests to be rejected

- EBS VolumeThroughputPercentage
- Elastic Load Balancer SpilloverCount

Q49)

Your company is being audited by a third party IT auditing service; they have asked you for details about the physical network and virtualization infrastructure.

What to you tell them? Choose the correct answer:

- ✅ You go to your AWS rep with the control in question and AWS will give the provided information to the third party in charge of doing your audit

Explanation:-You go to your AWS rep with the control in question and AWS will give the provided information to the third party in charge of doing your audit

- The audit does not apply to our us since we do not have control over AWS
- You print off details about the AWS infrastructure provided by the AWS infrastructure website
- You direct the auditing service to an AWS representative

Q50) Which of the following is a security best practice for an AWS environment? Choose the correct answer:

- ✅ Enable MFA on the root user for your AWS account and use IAM users rather than the root user for administrative tasks.

Explanation:-Enable MFA on the root user for your AWS account and use IAM users rather than the root user for administrative tasks. IAM user accounts should not be used for executing automated scheduled tasks on EC2 instances, and automated tasks do not use MFA. The default VPC is built for ease of use, not security. IAM user credentials should not be stored on AMIs; EC2 instances that need permission to perform actions on AWS resources should use IAM roles

- Enable MFA for all IAM user accounts that are used to execute automated scheduled tasks from EC2 instances.
- Use the default VPC provided by AWS for deploying your EC2 and RDS instances.
- Only store IAM user credentials on private AMIs.

Q51)

We have terminated an instance in which we have an EBS attached volume.

What do we do now if we need to access the important data that was on this volume if we created this instance with the default storage options? Choose the correct answer:

- Create multiple EBS volumes and replicate the data between them
- ✅ If we did not first take a snapshot of the EBS volume we will not be able to access the data after an instance termination

Explanation:-If we did not first take a snapshot of the EBS volume we will not be able to access the data after an instance termination By default, the EBS volumes are selected to terminate upon instance termination; however, when creating an EC2 instance we have the option to un-select the data deletion option. We must also create snapshots of the EBS volume which we can restore the data from

- We can restore the data from a snapshot
- AWS has high availability so our data is still available

Q52)

We have a two-tiered application with the following components. We have an ELB, three web/application servers on EC2, and one MySQL RDS database.

When our load grows, the database queries take longer and slow down the overall response time for the user request.

Which three options would we choose to speed up performance? Choose the 3 correct answers:

- ✅ We can cache our database queries with ElastiCache

Explanation:-We can shard the database and distribute the load between shards, We can create an RDS read-replica and redirect half of the database read requests to it, We can cache our database queries with ElastiCache

- We can use Amazon CloudFront to cache database queries
- ✅ We can create an RDS read-replica and redirect half of the database read requests to it

Explanation:-We can shard the database and distribute the load between shards, We can create an RDS read-replica and redirect half of the database read requests to it, We can cache our database queries with ElastiCache

- ✅ We can shard the database and distribute the load between shards

Explanation:-We can shard the database and distribute the load between shards, We can create an RDS read-replica and redirect half of the database read requests to it, We can cache our database queries with ElastiCache

---

Q53) A successful systems administrator probably does not need to know how to use a script for: Choose the correct answer:

- ✅ Automating backups of RDS databases

Explanation:-AWS offers automated backups of RDS, thus it is not a requirement to script this task.

- Creating OS-level metrics in CloudWatch
- Automating backups of EBS volumes

- Downloading software and updates from a repository to an EC2 instance

Q54) Which option below is part of a failover process for a Multi-AZ zone in an RDS instance? Choose the correct answer:

- Our failed RDS database instance reboots
- Answer not provided
- ✓ The DNS for our primary DB instance is switched to the standby DB instance
- The new DB instances we create are in the standby zone

Q55)

We have developed a mobile application that gets downloaded several hundred times a week.

What authentication method should we enable for the mobile clients to access images that are stored in an AWS S3 bucket that provides us with the highest flexibility and rotates the credentials? Choose the correct answer:

- IAM user per ever registered client with an IAM policy that grants S3 access to the respective bucket
- Set up S3 bucket policies with a conditional statement restricting IP address
- Use ACLs to restrict the access to the selects AWS accounts
- ✓ Identity Federation based on AWS STS using an AWS IAM policy for the respective S3 bucket

Q56)

You have multiple AWS users with access to an Amazon S3 bucket. These users have permission to add and delete objects.

If you wanted to prevent accidental deletions, what might you do to prevent these users from performing accidental deletions of an object? Choose the correct answer:

- ✓ You can use Amazon MFA for verification for deleting an object
- Creating a bucket policy that prevents accidental deletions
- Remove the ability for the user to delete
- Enable versioning on the bucket

Q57)

You maintain an application on AWS to provide development and test platforms for your developers. Currently, both environments consist of an m1.small EC2 instance.

Your developers notice performance degradation as they increase network load in the test environment.

How would you mitigate these performance issues in the test environment? Choose the correct answer:

- Configure Amazon CloudWatch to provision more network bandwidth when network utilization exceeds 80%
- ✓ Upgrade the m1.small to a larger instance type
- Add an additional ENU to the test instance
- Use the EBS optimized option to offload EBS traffic

Q58)

Your supervisor is concerned about losing read access to your RDS database in the unlikely event of an AWS regional failure.

You design a plan to create a read replica of the database in another region, but your supervisor sees a problem with this plan.

What problem does he see? Choose the correct answer:

- Replication requires VPC peering between the regions, and you have overlapping CIDR blocks in the two VPCs.
- AWS does not support RDS read replicas in different regions from the source database.
- Synchronous replication between the two regions will suffer from high latency.
- ✓ Your database is using PostgreSQL, which does not support cross-region replication.

Explanation:-Your database is using PostgreSQL, which does not support cross-region replication. Note: PostgreSQL on RDS now supports cross-region read replicas since June 2016, but please keep in mind that the exam probably won't be updated for a while. Read replicas are supported in different regions than the source RDS database, but only when using MySQL 5.6. You cannot synchronous replication between the two regions because, while latency is an important metric, read replicas use asynchronous replication, not synchronous replication. You cannot VPC peer between VPCs in different regions and because replication does not require VPC peering.

Q59)

You are uploading 3 gigabytes of data every night to S3 from your on-premises data center. It takes 3 hours to upload and you are uploading it to Amazon S3.

You are only using half of your available bandwidth through your internet provider.

How might you decrease the amount of time to back up that 3GB of data from your on-premises data center to S3? Choose the 2 correct answers:

- ✓ You could establish a Direct Connect connection between your on-premises data center and AWS VPC

Explanation:-You can use multipart upload to speed up the upload process, You could establish a Direct Connect connection between your on-premises data center and AWS VPC

- ✓ You can use multipart upload to speed up the upload process

Explanation:-You can use multipart upload to speed up the upload process, You could establish a Direct Connect connection between your on-premises data center and AWS VPC

- Increase your instance size
- Increase your provisioned IOPS

Q60)

Rule 100 in a NACL associated with subnets A and B denies HTTP traffic from 0.0.0.0/0. Rule 105 in the same NACL allows HTTP traffic from 0.0.0.0/0.

EC2 Instances in subnet A are associated with a security group that allows HTTP traffic from 192.168.0.0/24.

EC2 Instances in subnet B are associated with a security group that denies HTTP traffic from 128.168.0.0/24.

Which of the following statements are true? Choose the correct answer:

- HTTP traffic from 192.168.0.0/24 will be denied to EC2 instances in Subnet A because of the NACL rules.
- HTTP traffic from 192.168.0.0/24 will be allowed to EC2 instances in Subnet A.
- HTTP traffic from the internet will be allowed to EC2 instances in Subnet B.
- ✅ HTTP traffic from the internet will be denied to EC2 instances in both subnets due to the NACL rules.

Explanation:-HTTP traffic from the internet will be denied to EC2 instances in both subnets due to the NACL rules. Rule 105 is the higher number rule and will not be evaluated. NACL rules are evaluated in order from lowest to highest so HTTP traffic from the internet will be denied to instances in subnet B.

Q61)

You need to establish a secure backup and archiving solution for your company, using AWS.

Documents should be immediately accessible for three months and available for five years for compliance reasons.

Which AWS service fulfills these requirements in the most cost-effective way? Choose the correct answer:

- ✅ Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.

Explanation:-Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.

- Use StorageGateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.
- Use Direct Connect to upload data to S3 and use IAM policies to move the data into Glacier for long-term archiving.
- Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.

Q62) Which of the following CloudWatch metrics require a custom monitoring script to populate the metric? Choose the 2 correct answers:

- CPU
- CPU Utilization
- ✅ Swap Usage
- ✅ Available Disk Space

Q63) What AWS services allow you access to the underlying operating system? Choose the 3 correct answers:

- ✅ EC2
- RDS
- ✅ Hadoop
- ✅ Elastic BeanStalk

Q64)

A colleague noticed that CloudWatch was reporting that there had not been any connections to one of your MySQL databases for several months.

You decided to terminate the database.

Two months after the database was terminated, you get a phone call from a very upset user who needs information from that database to run end-of-year reports.

What can you do? Choose the correct answer:

- ✅ If you took a manual snapshot of the database, you can restore the database from that snapshot.

Explanation:-If you took a manual snapshot of the database, you can restore the database from that snapshot. Manual snapshots persist even after a database is terminated. There is not an expiration period for manual snapshots. While automated backups do have a maximum retention period of 35 days, they are deleted at the time a database is terminated

- Nothing, since the 35-day maximum retention period for automated backups has expired.
- You can restore the database from the most recent automated backup of the database.
- Nothing, since the 35-day maximum retention period for snapshots has expired.

Q65)

You are managing a large magazine application inside Amazon Web Services. Your company posts an article that gets picked up internationally, causing millions of visitors to hit your application.

Such a large increase in traffic causes strain on your DB server which is dynamically servicing the blog content.

How might you quickly resolve this issue and make the blog post infinitely scaleable? Choose the correct answer:

- ✅ Create a static HTML page using S3 and use Route 53 to point DNS to the static S3 bucket.

Explanation:-Create a static HTML page using S3 and use Route 53 to point DNS to the static S3 bucket.

- Increase the RDS instance size and enable Multi-AZ failover
- Enable Auto Scaling on the EC2 instances.
- Enable ElastiCache caching to helps serve the Dynamic content.