Which statement best describes Availability Zones?

Two zones containing compute resources that are designed to automatically maintain synchronized copies of each other's data.

Restricted areas designed specifically for the creation of Virtual Private Clouds.

Distinct locations from within an AWS region that are engineered to be isolated from failures.

A Content Distribution Network used to distribute content to users.

Distinct locations from within an AWS region that are engineered to be isolated from failures.

A new employee has just started work, and it is your job to give her administrator access to the AWS console. You have given her a user name, an access key ID, a secret access key, and you have generated a password for her. She is now able to log in to the AWS console, but she is unable to interact with any AWS services. What should you do next?

Grant her Administrator access by adding her to the Administrators' group.

Tell her to log out and try logging back in again.

Ensure she is logging in to the AWS console from your corporate network and not the normal internet.

Require multi-factor authentication for her user account.

Grant her Administrator access by adding her to the Administrators' group.

You are a solutions architect working for a large engineering company who are moving from a legacy infrastructure to AWS. You have configured the company's first AWS account and you have set up IAM. Your company is based in Andorra, but there will be a small subsidiary operating out of South Korea, so that office will need its own AWS environment. Which of the following statements is true?
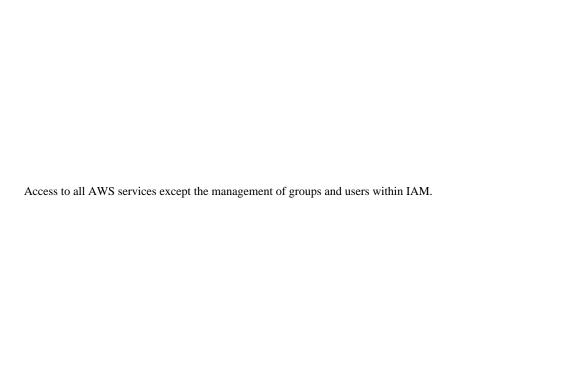
You will need to configure your policy documents regionally, however your users are global.

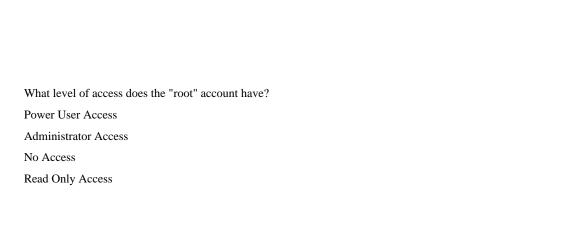You will then need to configure Users and Policy Documents for each region respectively.

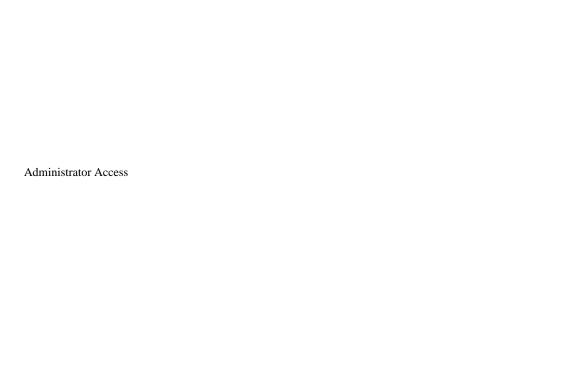You will need to configure your users regionally, however your policy documents are global.

You will need to configure Users and Policy Documents only once, as these are applied globally.

You will need to configure Users and Policy Documents only once, as these are applied globally.

Power User Access allows _____.

Access to all AWS services except the management of groups and users within IAM.

Users to inspect the source code of the AWS platform

Full Access to all AWS services and resources.

Read Only access to all AWS services and resources.

Access to all AWS services except the management of groups and users within IAM.

What level of access does the "root" account have?

Power User Access

Administrator Access

No Access

Read Only Access

Administrator Access

You are a security administrator working for a hotel chain. You have a new member of staff who has started as a systems administrator, and she will need full access to the AWS console. You have created the user account and generated the access key id and the secret access key. You have moved this user into the group where the other administrators are, and you have provided the new user with their secret access key and their access key id. However, when she tries to log in to the AWS console, she cannot. Why might that be?

You have not yet activated multi-factor authentication for the user, so by default they will not be able to log in.

You have not applied the "log in from console" policy document to the user. You must apply this first so that they can log in.

You cannot log in to the AWS console using the Access Key ID / Secret Access Key pair. Instead, you must generate a password for the user, and supply the user with this password and your organization's unique AWS console login URL.

Your user is trying to log in from the AWS console from outside the corporate network. This is not possible.

You cannot log in to the AWS console using the Access Key ID / Secret Access Key pair. Instead, you must generate a password for the user, and supply the user with this password and your organization's unique AWS console login URL.

What is the availability on RRS?

99.90%

99%

99.99%

100%

99.99%

How many S3 buckets can I have per account by default?

100

50

20

10

100

You work for a busy digital marketing company who currently store their data on premise. They are looking to migrate to AWS S3 and to store their data in buckets. Each bucket will be named after their individual customers, followed by a random series of letters and numbers. Once written to S3 the data is rarely changed, as it has already been sent to the end customer for them to use as they see fit. However on some occasions, customers may need certain files updated quickly, and this may be for work that has been done months or even years ago. You would need to be able to access this data immediately to make changes in that case, but you must also keep your storage costs extremely low. The data is not easily reproducible if lost. Which S3 storage class should you choose to minimise costs and to maximize retrieval times?

S3

S3 - IA

S3 - RRS

Glacier

S3 - IA

You work for a health insurance company that amasses a large number of patients' health records. Each record will be used once when assessing a customer, and will then need to be securely stored for a period of 7 years. In some rare cases, you may need to retrieve this data within 24 hours of a claim being lodged. Given these requirements, which type of AWS storage would deliver the least expensive solution?

S3 - RRS

S3 - IA

Glacier

S3

Glacier

What is AWS Storage Gateway?

None of the above.

It's an on-premise virtual appliance that can be used to cache S3 locally at a customers site.

It allows large scale import/exports in to the AWS cloud without the use of an internet connection.

It allows a direct MPLS connection in to AWS.

It's an on-premise virtual appliance that can be used to cache S3 locally at a customers site.

Which AWS CLI command should I use to create a snapshot of an EBS volume?

aws ec2 new-snapshot

aws ec2 create-snapshot

aws ec2 deploy-snapshot

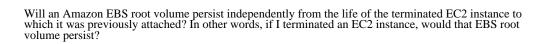aws ec2 fresh-snapshot

aws ec2 create-snapshot

Can I delete a snapshot of an EBS Volume that is used as the root device of a registered AMI?

No.

Only via the Command Line.

Yes.

Only using the AWS API.

No

I can use the AWS Console to add a role to an EC2 instance after that instance has been created and powered-up.
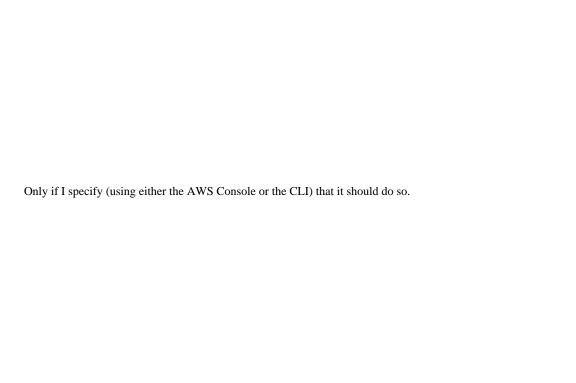
False

True

True

Will an Amazon EBS root volume persist independently from the life of the terminated EC2 instance to which it was previously attached? In other words, if I terminated an EC2 instance, would that EBS root volume persist?

Yes.

Only if I specify (using either the AWS Console or the CLI) that it should do so.

It depends on the region in which the EC2 instance is provisioned.

No.

Only if I specify (using either the AWS Console or the CLI) that it should do so.

True or False: There is a limit to the number of domain names that you can manage using Route 53.

True and False. With Route 53, there is a default limit of 50 domain names. However, this limit can be increased by contacting AWS support.

True. There is a hard limit of 10 domain names. You cannot go above this number.

False. By default, you can support as many domain names on Route 53 as you want.

True and False. With Route 53, there is a default limit of 50 domain names. However, this limit can be increased by contacting AWS support.

Does Route53 support MX Records?

No

Yes

Only in Us-West-1

Only if they have an SPF record

Yes

Route53 does not support zone apex records (naked domain names).

It depends on the configuration.

False.

Only in Us-East-1.

True.

False.

What happens to the I/O operations of a single-AZ RDS instance during a database snapshot or backup?

I/O operations to the database are sent to a Secondary instance of a Multi-AZ installation (for the duration of the snapshot.)

I/O operations will function normally.

I/O may be briefly suspended while the backup process initializes (typically under a few seconds), and you may experience a brief period of elevated latency.

Nothing.

I/O may be briefly suspended while the backup process initializes (typically under a few seconds), and you may experience a brief period of elevated latency.

Which AWS DB platform is most suitable for OLTP?

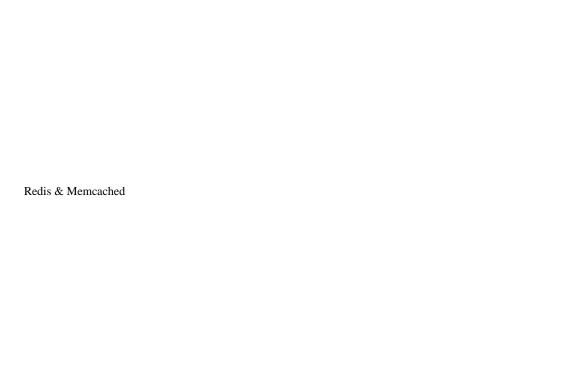Redshift

RDS

DynamoDB

ElastiCache

RDS

When you add a rule to an RDS security group, you must specify a port number or protocol.

False

True

False

Amazon's ElastiCache uses which two engines?

Redis & Memory

Reddit & Memcrush

MyISAM & InnoDB

Redis & Memcached

Redis & Memcached

If you are using Amazon RDS Provisioned IOPS storage with a MySQL or Oracle database engine, what is the maximum size RDS volume you can have by default?

6TB

3TB

500GB

1TB

6TB

Security groups act like a firewall at the instance level, whereas _____ are an additional layer of security that act at the subnet level

Network ACLs

VPC Security Groups

DB Security Groups

Route Tables

Network ACLs

By default, how many VPCs am I allowed in each AWS Region?
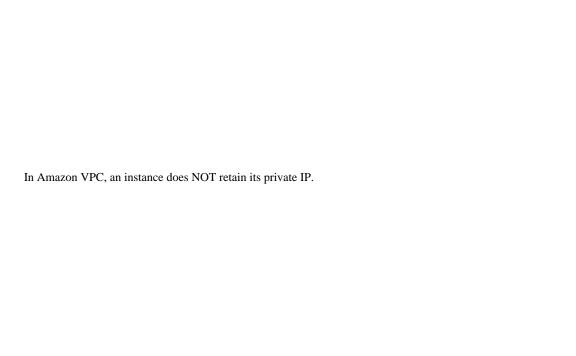
1

6

5

2

5

Select the incorrect statement.

In Amazon VPC, an instance does NOT retain its private IP.

You may have only 1 internet gateway per VPC.

It is possible to have private subnets in VPC.

In Amazon VPC, an instance retains its private IP.

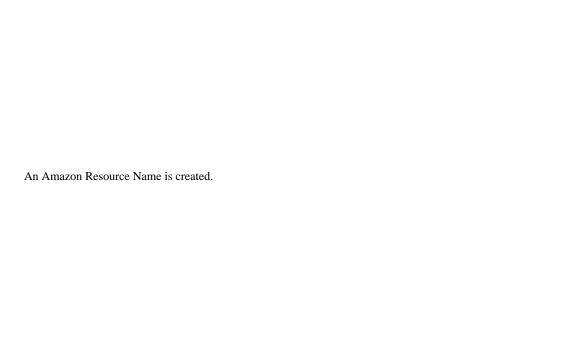In Amazon VPC, an instance does NOT retain its private IP.
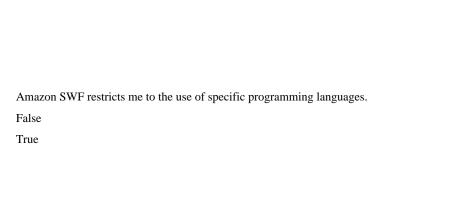
What happens when you create a topic on Amazon SNS?

You cannot create a topic on SNS.

The topic will terminate your EC2 instances that aren't identified by tags.

Nothing, as topics are specific to Amazon SQS.

An Amazon Resource Name is created.

An Amazon Resource Name is created.

Amazon SWF restricts me to the use of specific programming languages.

False

True

False

In RDS, you are responsibly for maintaining the OS, application security patching, antivirus, etc.

True

False

False

When deploying databases on your EC2 instances, AWS recommends that you deploy on magnetic storage rather than SSD storage if you need better performance.

False

True

False

Individual instances are provisioned _____.

Globally

In Availability Zones

In Regions

In Availability Zones

In RDS, what is the maximum storage size for a Microsoft SQL Server instance running SQL Server Express edition?

300GB

4TB

1TB

10GB

300 Gb
There are two different limits -- that of the DB (10GB), and that of the DB instance server storage (300GB). A DB server instance could quite easily host several DBs, or a DB and support files such as logs, dumps, and flat file backups. Please see the AWS documentation for full details. Further information:

If an Amazon EBS volume is an additional partition (not the root volume), can I detach it without stopping the instance?

No, you will need to stop the instance.

Yes, although it may take some time.

Yes, although it may take some time.

In RDS, what is the maximum value I can set for my backup retention period?

45 Days

15 Days

35 Days

30 Days

35 Days

What is the underlying Hypervisor for EC2?

ESX

OVM

Hyper-V

Xen

Xen

What is the maximum response time for a Business Level Premium Support Case?

1 Hour

1 Day

12 Hours

15 Minutes

1 Hour

What are the four levels of AWS premium support?

Free, Bronze, Silver, and Gold

Basic, Developer, Business, and Enterprise

It's an IAAS platform, so there is no support.

Basic, Startup, Business, and Enterprise

Basic, Developer, Business, and Enterprise

Can I move a reserved instance from one region to another?

No.

Only in the US.

Yes.

It depends on the region.

No.

The AWS platform consists of how many regions?

12

16

15

14

MySQL installations default to port number _____.

80

1433

3389

3306

3306

If I wanted to run a database on an EC2 instance, which of the following storage options would Amazon recommend?

RDS
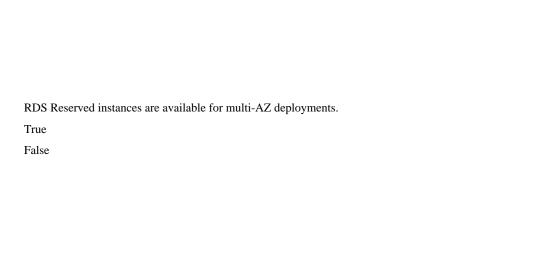
EBS

S3

Glacier

EBS

Amazon RDS does not currently support increasing storage on an active _____ Db instance.

SQL Server

MySQL

Aurora

Oracle

MySQL

When I create a new security group, all outbound traffic is allowed by default.

True

False

True

RDS Reserved instances are available for multi-AZ deployments.

True

False

True

With new RDS Db instances, automated backups are enabled by default?

False

True

True

To save administration headaches, Amazon recommends that you leave all security groups in web facing subnets open on port 22 to 0.0.0.0/0 CIDR. That way, you can connect where ever you are in the world.

False

True

False

How many copies of my data does RDS - Aurora store by default?

3

2

1

6

You can RDP or SSH in to an RDS instance to see what is going on with the operating system.

False

True

False

Which of the following statements are true about Docker containers on AWS? (Choose 4)

To use private images in ECS, you must refer to Docker images from ECR.

You must use ECS to manage running Docker containers in AWS.

ECR can be used to store Docker images.

You can use the ECS Agent without needing to use ECS.

You can have AWS manage Kubernetes for you.

ECS allows you to control the scheduling and placement of your containers and tasks.

You can install and manage Kubernetes on AWS, yourself.

To be able to use ECS, you must use the ECS Agent.

You must use ECS to manage running Docker containers in AWS.

ECR can be used to store Docker images.

ECS allows you to control the scheduling and placement of your containers and tasks.

You can install and manage Kubernetes on AWS, yourself.

To be able to use ECS, you must use the ECS Agent.

You have launched a NAT instance in to a public subnet, and you have configured all relevant security groups, network ACLs, and routing policies to allow this NAT to function. However, EC2 instances in the private subnet still cannot communicate out to the internet. What troubleshooting steps should you take to resolve this issue?

Configure all traffic to go out via the Elastic Load Balancer.

Enable Source/Destination Check on the NAT instance.

Disable the Source/Destination Check on your NAT instance.

Update Route53 to allow traffic to flow out from your VPC.

Disable the Source/Destination Check on your NAT instance.

Due to international monetary regulations issued by the IMF, a large multi-national banking organization requires that all their Australian customers' data must not leave the Australian jurisdiction. Similarly, all Japanese customers' data may not leave the Japanese jurisdiction without explicit permission from the IMF. While registering, a user must include their residential address as part of their user profile. What steps should be taken to enforce these regulations on a web-based application running on EC2?

Run Amazon EC2 instances in multiple AWS Availability Zones in a single region, and leverage an elastic load balancer with session stickiness to route traffic to the appropriate zone based on a users profile.

Deploy your application on multiple EC2 instances in multiple regions. Then, use Route 53s latency-based routing capabilities to route traffic to the appropriate region based on a users latency.

Due to the strict regulations, you should use a third party data provider to verify the users location based on their profile. It would not be appropriate to rely on latency based routing, as this would not always be 100% accurate.

Deploy your application on EC2 instances in multiple regions, and then use an elastic load balancer with session stickiness to route traffic to the appropriate region based on a users profile country.

Due to the strict regulations, you should use a third party data provider to verify the users location based on their profile. It would not be appropriate to rely on latency based routing, as this would not always be 100% accurate.
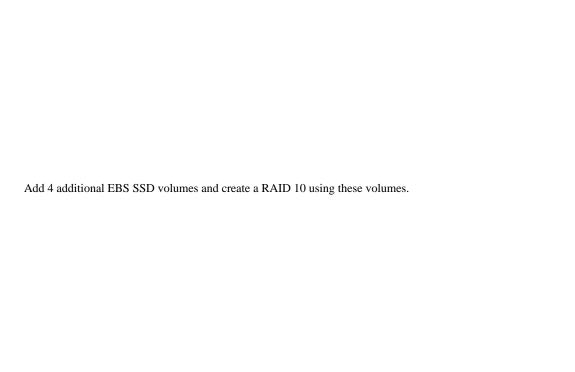
You are hosting a MySQL database on the root volume of an EC2 instance. The database is using a large number of IOPS, and you need to increase the number of IOPS available to it. What should you do?

Use Cloud Front to cache the database.

Migrate the database to an S3 bucket.

Add 4 additional EBS SSD volumes and create a RAID 10 using these volumes.

Migrate the database to Glacier.

Add 4 additional EBS SSD volumes and create a RAID 10 using these volumes.

You have created a new subdomain for your popular website, and you need this subdomain to point to an Elastic Load Balancer using Route53. Which DNS record set should you create?

AAAA

A

MX

CNAME

CNAME

By default, new subnets in a custom VPC can communicate with each other across Availability Zones.

False

True

True

Until recently, your company has been running each of your application's many microservices as separate Elastic Beanstalk instances. But your developers have just changed those from deploying and running code directly to now deploying and running Docker containers, instead. Which of the following options would make the most efficient use of AWS resources? (Choose 2)

Use the Elastic Container Runner service to auto-scale the number of running service containers based on load.

Package the containers so they can be deployed using Lambda, to take advantage of its pay-for-use model.

Create an ECS cluster and configure it to run the different microservice containers across the hosts.

Set up Elastic Beanstalk to most efficiently orchestrate running all the containers across a single auto-scaled group of instances

Use ECS with Docker for Windows to make use of your overprovisioned and underutilized ASP.Net reserved instances.

Create an auto-scaled group of EC2 instances and run Kubernetes across them to orchestrate the containers.

Create an ECS cluster and configure it to run the different microservice containers across the hosts.

Create an auto-scaled group of EC2 instances and run Kubernetes across them to orchestrate the containers.

How should you direct traffic to an ECS cluster running three microservices with the following URLs: 'https://services.mydomain.com/ServiceA/', 'https://services.mydomain.com/ServiceB/', 'https://anotherservice.mydomain.com/'?

Use Route53 to send the requests to the right containers.

Use an Application Load Balancer with cross-zone load balancing on.

Use an Application Load Balancer with cross-zone load balancing off.

Send the requests to the ECS instances and they will route the traffic.

Use a Classic Load Balancer with cross-zone load balancing off.

Use a Classic Load Balancer with cross-zone load balancing on.

ALBs allow you to set up multiple targets and route to them based on the path and/or hostname. (Previously, ALBs couldn't direct traffic based on the hostname, but they now can.) Further information:

Amazon S3 buckets in all regions other than "US Standard" provide read-after-write consistency for PUTS of new objects.

False

True

True
US STANDARD is a redundant term. The AWS exams still use the term, so you need to be familiar with it. The questions is still valid just ignore the reference to US STANDARD and any past discrepancies that may have existed. Further information:

An application saves the logs to an S3 bucket. A user wants to keep the logs for one month for troubleshooting purposes, and then purge the logs.
What feature will enable this?
A. Adding a bucket policy on the S3 bucket.
B. Configuring lifecycle configuration rules on the S3 bucket.
C. Creating an IAM policy for the S3 bucket.
D. Enabling CORS on the S3 bucket.

B. Configuring lifecycle configuration rules on the S3 bucket.

An organization is building an Amazon Redshift cluster in their shared services VPC. The cluster will host sensitive data.

How can the organization control which networks can access the cluster?

A. Run the cluster in a different VPC and connect through VPC peering.

B. Create a database user inside the Amazon Redshift cluster only for users on the network.

C. Define a cluster security group for the cluster that allows access from the allowed networ

C

A security group can grant access to traffic from the allowed networks via the CIDR range for each network. VPC peering and VPN are connectivity services and cannot control traffic for security. Amazon Redshift user accounts address authentication and authorization at the user level and have no control over network traffic.
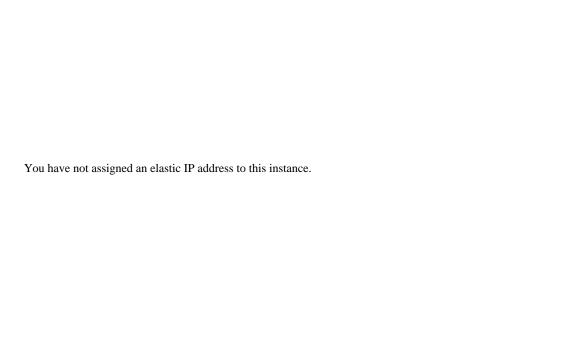
You work for a construction company that has their production environment in AWS. The production environment consists of 3 identical web servers that are launched from a standard Amazon linux AMI using Auto Scaling. The web servers are launched in to the same public subnet and belong to the same security group. They also sit behind the same ELB. You decide to do some testing: you launch a 4th EC2 instance into the same subnet and same security group. Annoyingly, your 4th instance does not appear to have internet connectivity. What could be the cause of this?

You have not configured a NAT in the public subnet.

You need to update your route table so as to provide a route out for this instance.

You have not assigned an elastic IP address to this instance.

You have not configured a routable IP address in the host OS of the fourth instance.

You have not assigned an elastic IP address to this instance.

You work in the genomics industry, and you process large amounts of genomic data using a nightly Elastic Map Reduce (EMR) job. This job processes a single 3 Tb file which is stored on S3. The EMR job runs on 3 on-demand core nodes and four on-demand task nodes. The EMR job is now taking longer than anticipated, and you have been asked to advise how to reduce the completion time. Which of the following would you suggest?

Store the file on Elastic File Service instead of S3, then mount EFS as an independent volume for your core nodes.

Configure an independent VPC in which to run the EMR jobs, then mount EFS as an independent volume for your core nodes.

Use four Spot Instances for the task nodes rather than four On-Demand instances.

You should reduce the input split size in the MapReduce job configuration, then adjust the number of simultaneous mapper tasks so that more tasks can be processed at once.

You should reduce the input split size in the MapReduce job configuration, then adjust the number of simultaneous mapper tasks so that more tasks can be processed at once.

Your company has decided to set up a new AWS account for test and dev purposes. They already use AWS for production, but would like a new account dedicated for test and dev so as to not accidentally break the production environment. You launch an exact replica of your production environment using a CloudFormation template that your company uses in production. However, CloudFormation fails. You use the exact same CloudFormation template in production, so the failure is something to do with your new AWS account. The CloudFormation template is trying to launch 60 new EC2 instances in a single availability zone. After some research you discover that the problem is _____.

Your CloudFormation template is configured to use the parent account and not the new account. Change the account number in the CloudFormation template and relaunch the template.

For all new AWS accounts, there is a soft limit of 20 EC2 instances per availability zone. You should submit the limit increase form and retry the template after your limit has been increased.

For all new AWS accounts, there is a soft limit of 20 EC2 instances per region. You should submit the limit increase form and retry the template after your limit has been increased.

You cannot launch more than 20 instances in your default VPC. Instead, reconfigure the CloudFormation template to provision the instances in a custom VPC.
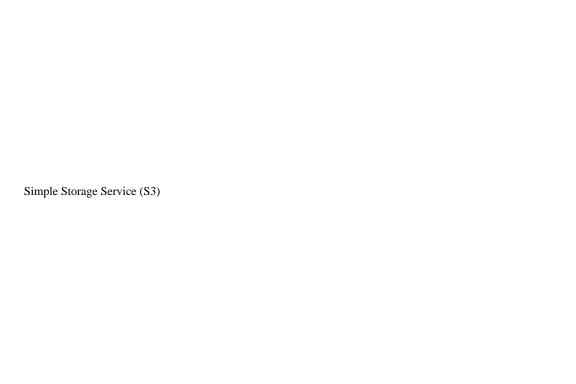
For all new AWS accounts, there is a soft limit of 20 EC2 instances per region. You should submit the limit increase form and retry the template after your limit has been increased.

You have been asked to identify a service on AWS that is a durable key value store. Which of the services below meets this definition?

Mobile Hub

Kinesis

Elastic File Service (EFS)

Simple Storage Service (S3)
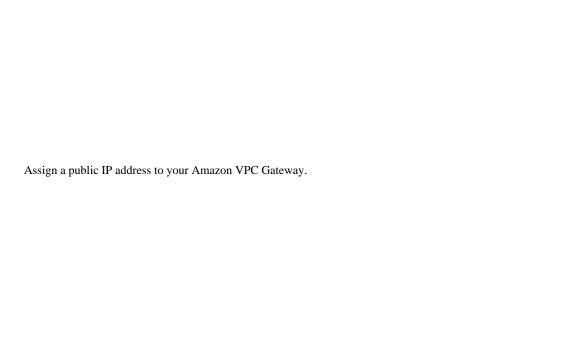
Simple Storage Service (S3)

You work for a famous bakery who are deploying a hybrid cloud approach. Their legacy IBM AS400 servers will remain on premise within their own datacenter. However, they will need to be able to communicate to the AWS environment over a site-to-site VPN connection. What do you need to do to establish the VPN connection?

Connect to the environment using AWS Direct Connect.

Assign a public IP address to your Amazon VPC Gateway.

Create a dedicated NAT and deploy this to the public subnet.

Update your route table to add a route for the NAT to 0.0.0.0/0.

Assign a public IP address to your Amazon VPC Gateway.

Which of the following services should you implement in multiple availability zones in order to achieve high availability? (Choose 2)

Simple Queue Service

EC2

RDS

Simple Storage Service

DynamoDB

EC2
RDS

The Customer Experience manager comes to see you about some odd behaviours with the ticketing system: messages presented to the support team are not arriving in the order in which they were generated. You know that this is due to the way that the underlying SQS standard queue service is being used to manage messages. Which of the following are correct explanations? (Choose 2)

The support staff are probably using the provided admin tools to amend the priority in the SQS queue based on their experience and insights about the issues.

SQS has been setup to prioritize messages in the queue based on keywords.

As the SQS service gets busy, some of the hosts will automatically swap from FIFO to LIFO to provide a better work load balance and clearance rate.

SQS uses multiple hosts, and each host holds only a portion of all the messages. When a staff member calls for their next message, the consumer process does not see all the hosts or all the messages. As such, messages are not necessarily delivered in the order in which they were generated.

If an agent abandons a message or takes a break before finishing with a message, it will be offered in the queue again. In order to ensure that no message is lost, a message will persist in the SQS queue until it is processed successfully.

SQS uses multiple hosts, and each host holds only a portion of all the messages. When a staff member calls for their next message, the consumer process does not see all the hosts or all the messages. As such, messages are not necessarily delivered in the order in which they were generated.

If an agent abandons a message or takes a break before finishing with a message, it will be offered in the queue again. In order to ensure that no message is lost, a message will persist in the SQS queue until it is processed successfully.

In which of the following ways can security privileges be granted to Docker containers? (Choose 2)

Role granted to an ECS Cluster

Role granted to an ECS Task

Role granted to a single running container in ECS

Image in ECR

Role granted to an ECS Service

Role granted to ECS Container Instances

Role granted to an ECS Task
Role granted to ECS Container Instances

Which of the following are valid S3 data encryption options? (Choose 4)

A client library such as Amazon S3 Encryption Client.

Open SSL.

Server Side Encryption (SSE)-S3.

SSE-C.

SSE-KMS.

A client library such as Amazon S3 Encryption Client.

Server Side Encryption (SSE)-S3.

SSE-C.

SSE-KMS.

To establish a successful site-to-site VPN connection from your on-premise network to an AWS Virtual Private Cloud, which of the following must be configured? (Choose 3)

A private subnet in your VPC

A VPC with Hardware VPN Access

A Virtual Private Gateway

A NAT instance

An on-premise Customer Gateway

A VPC with Hardware VPN Access

A Virtual Private Gateway

An on-premise Customer Gateway

You have three AWS accounts (A, B & C) which share data. In an attempt to maximize performance between the accounts, you deploy the instances owned by these three accounts in 'eu-west-1b'. During testing, you find inconsistent results in transfer latency between the instances. Transfer between accounts A and B is excellent, but transfers between accounts B and C, and C and A, are slower. What could be the problem ?

The names of the AZs are randomly applied, so "eu-west-1b" is not necessarily the same physical location for all three accounts.

Account C has been allocated to an older section of the Data Hall with slower networking.

The instances for Account C are on an overloaded Host. Stop all the Account C instances and then start them together so that they run an a new host.

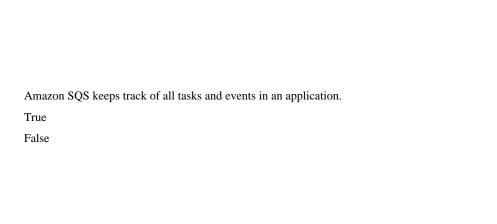You have accidentally set up account C in "us-west-1b".

You have incorrectly configured the cross-account authentication policies in Account C, adding latency to those instances.

Sorry!
Availability Zone names are unique per account and do not represent a specific set of physical resources.
Further information: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

Amazon SQS keeps track of all tasks and events in an application.

True

False

F
With SQS, you must implement your own application-level tracking, especially if your application uses multiple queues. Amazon SWF does provide tracking of these types. Further information: https://aws.amazon.com/swf/details/

Your company has just purchased another company. As part of the merger, your team has been instructed to cross connect the corporate networks. You run all your confidential corporate services and Internal DNS in a VPC. The merged company has all their confidential corporate services and Internal DNS on-premises. After establishing a Direct-Connect service between your VPC and their on-premise network, and confirming all the routing, firewalls, and authentication, you find that while you can resolve names against their DNS, the other company services is unable to resolve names against your DNS servers. Why might this be?

Route53 is not an industry standard DNS service, and zone transfers and name resolution must be done via a proprietary API.

By design, AWS DNS does not respond to requests originating from outside the VPC.

The computers are not configured properly. You need to add the IP address of the AWS DNS servers into the DNS options of the IP stack.

You cannot use DNS in this way. You need to merge the zones under a parent zone registered with ICANN.

AWS Route53 is an Internet service, and the other company needs to do lookups and zone transfers via the Internet, not the Direct-Connect link.

2
Route53 has a security feature that prevents internal DNS from being read by external sources. The work around is to create a EC2 hosted DNS instance that does zone transfers from the internal DNS, and allows itself to be queried by external servers.

Which of the following strategies does AWS use to deliver the promised levels of DynamoDB performance? (Choose 2)

DynamoDB instances can be configured with EBS-Optimised connections.

The Database is partitioned across a number of instances.

AWS deploys Read Replicas of the database to balance the load.

AWS deploy caching instances in front of the DynamoDB cluster.

Data is stored on Solid State Disks.

B,E
there is no magic, just fast hardware and dynamic DB sharding. . Further information

Your Security Manager has hired a security contractor to audit your firewall implementation. When the consultant asks for the login details for the firewall appliance, which of the following might you do? (Choose 2)

Create an IAM Role with a policy that can Read Security Group and nACL settings.

Explain that AWS is a cloud service and that AWS manages the Network appliances.

Create an IAM User with a policy that can Read Security Group and Route settings.

Create an IAM Role with a policy that can Read Security Group and Route settings.

Create an IAM User with a policy that can Read Security Group and nACL settings.

Explain that AWS implements network security differently and that there is no such thing as a Firewall appliance. You might then suggest that the consultant take the 'A Cloud Guru' AWS CSA-A course in preparation for the audit.

E,F

AWS has removed the Firewall appliance from the hub of the network and implemented the firewall functionality as stateful Security Groups, and stateless subnet NACLs. This is not a new concept in networking, but rarely implemented at this scale. Further information:

Your client has been experiencing problems with his aging in-house infrastructure, and is extremely concerned about managing the cost of maintaining his online presence. After deciding that the cost of developing a sound DR plan more than makes up for the negative impact of being off-line, the board has directed you to prepare a proposal that achieves an RTO of 20 hours, an RPO of 1 hour, and keeps the costs of meeting those target time-windows to a minimum. They have also mandated the use of the AWS Storage Gateway to mitigate the risk associated with a catastrophic NAS failure. Which of the following solutions best meet the requirements?
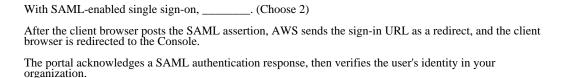
Work with the customer's engineers to identify the key servers and data. Help them setup an AWS account with IAM users, groups, and roles. Build templates of the critical web/app servers and save these as AMIs. Agree upon RDS specifications that meet the stated requirements. Set up the Storage Gateway and the Snapshot schedule to meet the RPO. Document, script, or automate the steps to initiate the RDS instance, the EC2 instances, the steps to restore the latest data from the Storage Gateway snapshots into RDS, plus any DNS changes. Test the process with each of the Operations team shifts.

Provide their engineering staff with an AWS account and create IAM Users, Groups, & Roles. Use CloudFormation/CloudFormer to clone the existing on-premises environment and store the build scripts in GitHub. Migrate the in-house DNS to Route53 to simplify cut-over. Set up the Storage Gateway and the Snapshot schedule to meet the RPO. Provide the engineering team with a CLI script to kick-start the CloudFormation build and restoration of the StorageGateway snapshots.

Provide their engineering staff with an AWS account, and ask them to rebuild all the servers in AWS to form a fully functional Hot Standby environment. Use Storage Gateway to copy the data on the NAS to S3 so that it can be accessed by the database servers.

Provide their engineering staff with an AWS account. Create a small, under-sized DR DB instance and use application synchronization to keep the DR instance synchronized within 30 seconds of the production instance. Build one of each web/app server and keep these patched and on-line. Provide the Ops team with written instructions explaining how to upgrade the DB host to a full sized instance within 20 minutes.

A
There are three key aspects: RTO, RPO, and cost. All three must be balanced and meet objectives for the design to be considered acceptable.

With SAML-enabled single sign-on, _____. (Choose 2)

After the client browser posts the SAML assertion, AWS sends the sign-in URL as a redirect, and the client browser is redirected to the Console.

The portal acknowledges a SAML authentication response, then verifies the user's identity in your organization.

The portal first verifies the user's identity in your organization, then generates a SAML authentication response.

The client browser is immediately directed to the AWS Console.

After the client browser posts the SAML assertion, AWS sends the sign-in URL as a redirect, and the client browser is redirected to the Console.

The portal first verifies the user's identity in your organization, then generates a SAML authentication response.

When making use of ec2 instances on Dedicated Hosting, which of the following modes are you able to transition between by stopping the instance and starting it again? (Choose 2)

Host & Default

Default & Dedicated

Dedicated & Default

Dedicated & Host

Host & Dedicated.

Dedicated & Host

Host & Dedicated.

The tenancy of an instance can only be change between variants of 'dedicated' tenancy hosting. It cannot be changed from or to default tenancy hosting. Further information:

Although your application customarily runs at 30% usage, you have identified a recurring usage spike (>90%) between 8pm and midnight daily. What is the most cost effective way to scale your application to meet this increased need?
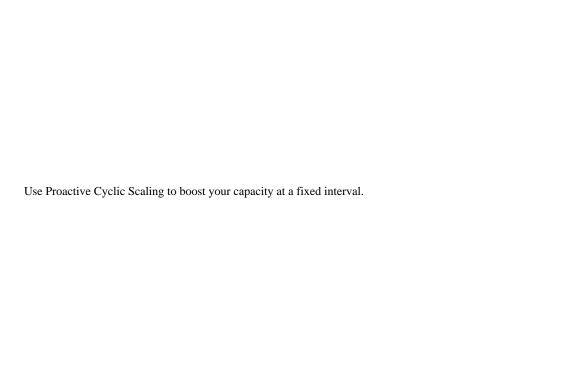
Increase the size of the Resource Group to meet demand.

Deploy additional EC2 instances to meet the demand.

Use Proactive Cyclic Scaling to boost your capacity at a fixed interval.

Manually deploy Reactive Event-based Scaling each night at 7:45.

Use Proactive Cyclic Scaling to boost your capacity at a fixed interval.

You work for a large media organization who has traditionally stored all their media on large SAN arrays. After evaluating AWS, they have decided to move their storage to the cloud. Staff will store their personal data on S3, and will have to use their Active Directory credentials in order to authenticate. These items will be stored in a single S3 bucket, and each staff member will have their own folder within that bucket named after their employee ID. Which of the following steps should you take in order to help set this up? (Choose 3)
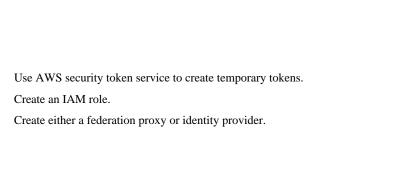
Create an IAM user for each member of staff and use their existing active directory password for the account.

Use AWS security token service to create temporary tokens.

Create an IAM role.

Create either a federation proxy or identity provider.

Tag each folder with the staff members ID.

Use AWS security token service to create temporary tokens.

Create an IAM role.

Create either a federation proxy or identity provider.

You are a consultant planning to deploy DynamoDB across three AZs. Your lead DBA is concerned about data consistency. Which of the following do you advise the lead DBA to do?

To ask the development team to code a Lambda function to check data consistency after each write.

To ask the development team to code for strongly consistent reads. As the consultant, you will advise the CTO of the increased cost.

To ask the development team to code to check for a successful completion code (200) at the completion of every write.

To ask the development team to implement a checksum algorithm to confirm that the data is consistent across all the AZs.

To ask the development team to code for Strongly Consistent Reads, as it will impact the read times slightly, but not the budget.

To ask the development team to code an maintenance task to run on a schedule to check consistency.

To ask the development team to code for strongly consistent reads. As the consultant, you will advise the CTO of the increased cost.

You have created a bespoke VPC that contains 2 web servers. These web servers must be publicly accessible by the internet and should also be highly resilient. Which of the following configurations should you consider? (Choose 2)

Setup an Elastic Load Balancer and place your 2 webservers behind this ELB in different Availability Zones. Configure a Route53 CNAME to use the public DNS address of the Elastic Load Balancer.

Setup an Elastic Load Balancer and place your 2 webservers behind this ELB in different Availability Zones. Configure a Route53 "A" record to point to the IP address of the Elastic Load Balancer.

Configure a NAT instance within your VPC. Create a route via the NAT and associate it with all private subnets within your VPC. Create a Route53 "A" record to point to the public IP address of the NAT.

Assign each EC2 instance with an Elastic IP Address. Configure Route53 with both EIP's and setup health checks with DNS failover.

A,D
You have the option of either using an Elastic Load Balancer or multiple Elastic IP addresses and configuring DNS failover with health checks using route 53. You cannot configure a Route53 A record that points to an ELB and you can't use a NAT as a makeshift Load Balancer.

You have been engaged by a company to design and lead the migration to an AWS environment. An argument has broken out about how to meet future Backup & Archive requirements and how to transition. The Security Manager and CTO are concerned about backup continuity and the ability to continue to access old archives. The Senior engineer is adamant that there is no way to retain the old backup solution in the AWS environment, and that they will lose access to all the current archives. What information can you share that will satisfy both parties in a cost effective manner? (Choose 2)

Meet with both parties and brief them on the AWS Storage Gateway VTL solution. Explain that it can initially be installed in the on-premises environment utilizing the existing enterprise backup product to start the transition without losing access to the existing backups and archives. Over the duration of the migration, most (if not all) the backup cycles will be replaced by the new VTL & VTS tapes.

Suggest that after transition, the AWS Storage Gateway VTL solution could be re-commissioned in a partner data centre retaining the existing equipment and maintaining access to the existing archives.

Meet with the Management team and explain that the Senior Engineer is correct: there is no mechanism for retaining the existing backup/archive solution as the AWS data centers are closed facilities.

Propose using the AWS Import/Export service to import the contents of the backup and archive tapes into S3/Glacier to preserve them in case they are required later.

Suggest that during transition a 2nd AWS Storage Gateway VTL solution could be commissioned in the customer's new VPC and integrated with existing VTS. At the same time, the existing Enterprise Backup Solution could be used to perform tape-to-tape copies to migrate the Archives from tape to VTL/VTS virtual tape

Propose that after transition access to Archive tapes could be managed via a 3rd party service provider for the odd occasion that a historic archive is required.

1,5
Any migration project needs to consider how to manage legacy data and data formats. This includes backup and archives. A 3rd party archive service is viable, but would be an ongoing expense.

You successfully configure VPC Peering between VPC-A and VPC-B. You then establish an IGW and a Direct-Connect connection in VPC-B. Can instances in VPC-A connect to your corporate office via the Direct-Connect service, and connect to the Internet via the IGW?

Instances in VPC-A will be able to access the Internet, but not the corporate office.

VPC peering does not support edge to edge routing.

Yes: VPC Peering is designed to route traffic between the VPCs.

Instances in VPC-A will be able to access the corporate office, but not the Internet.

VPC peering only routes traffic between source and destination VPCs. VPC peering does not support edge to edge routing

You work for a genomics company that is developing a cure for motor neuron disease by using advanced gene therapies. As a part of their research, they take extremely large data sets (usually in the terabytes) and analyze these data sets using Elastic Map Reduce. In order to keep costs low, they run the analysis for only a few hours in the early hours of the morning, using spot instances for the task nodes. The core nodes are on-demand instances. Lately however the EMR jobs have been failing. This is due to spot instances being unexpectedly terminated. Which of the following remedies would both keep costs manageable and mitigate the issues caused by terminated spot instances? (Choose 2)

Increase the bid price for the task nodes so that you have a greater threshold before the task nodes are terminated.

Increase the bid price for the core nodes.

Change the task nodes to on-demand instances.

Change the core nodes to spot instances and lower the spot price.

1,3

You should consider either increasing the bid price for the task nodes so that your nodes are not terminated or even converting the task nodes to on demand instances so as to ensure they are not prematurely terminated.

At the monthly product meeting, one of the Product Owners proposes an idea to address an immediate shortcoming of the product system: storing a copy of the customer price schedule in the customer record in the database. You know that you can store large text or binary objects in DynamoDB. You give a tentative OK to do a Minimal Viable Product test, but stipulate that it must comply with the size limitation on the Attribute Name & Value. Which is the correct limitation?

The combined Value and Name combined must not exceed 500 KB.

The combined Value and Name combined must not exceed 255 KB.

The Name must not exceed 64 KB and the Value must not exceed 255 KB.

The Name must not exceed 64 KB and the Value must not exceed 400 KB.

The Name must not exceed 64 KB and the Value must not exceed 500 KB.

The combined Value and Name combined must not exceed 400 KB.

DynamoDB allows for the storage of large text and binary objects, but there is a limit of 400 KB. Further information:

Your company has hired a young and enthusiastic accountant. After reviewing the AWS documentation and usage graphs, he announces that you are wasting vast amounts of money running servers for a full hour instead of spinning them up only when they are needed and down again as soon as they are idle for 1 minute. He cites the AWS claim that you only pay for what you use, and that as a senior engineer, you should be more conscious of wasting company money. How do you respond?

You leap across the meeting table and slap him for insulting you in front of your peers.

You thank him for his concern, and advise him that he has misinterpreted the pricing document: Instances are billed by the full hour, and partial hours are billed as such. Additionally, storage charges are incurred even if the Db instance sits idle. Taking into account productivity losses, stopping and restarting Db instances may actually result in additional costs. As such, your solution is fine as it now stands.

You grudgingly acknowledge his point and change your scheduling and tuning settings.

You acknowledge the problem and propose that you could downsize the instances so that the workload over the hour consumes the full instance capacity for the full hour. You might also propose closer monitoring and automation to allow you to up-size and down-size the instance each hour over the day to match the instance performance to the anticipated workload.

You thank him for his concern, and advise him that he has misinterpreted the pricing document: Instances are billed by the full hour, and partial hours are billed as such. Additionally, storage charges are incurred even if the Db instance sits idle. Taking into account productivity losses, stopping and restarting Db instances may actually result in additional costs. As such, your solution is fine as it now stands.

You have a database-style application that frequently has multiple reads and writes across the data set. Which of the following AWS storage services are capable of hosting this application? (Choose 2)

Glacier

S3

EBS

Elastic File Service (EFS)

EBS

Elastic File Service (EFS)

Your server logs are full of what appear to be application-layer attacks, so you deploy AWS Web Application Firewall. Which of the following conditions may you set when configuring AWS WAF? (Choose 3)

Termination Conditions

SQL Rejection Match Conditions

Size Constraint Conditions

IP Match Conditions

URL Match Conditions

String Match Conditions

Size Constraint Conditions

IP Match Conditions

String Match Conditions

If you don't use one of the AWS SDKs, you can perform DynamoDB operations over HTTP using the POST request method. The POST method requires you to specify the operation in the header of the request and provide the data for the operation in JSON format in the body of the request. Which of the following are valid DynamoDB Headers attributes? (Choose 4)

x-amz-date

x-amz-target

host

MD5-Hash

content-type

x-amz-meta-

x-amz-date

x-amz-target

host

content-type

You are running a media rich website with a global audience in US-EAST-1 for a customer in the publishing industry. The website updates every 20 minutes. The web-tier of the site sits on three EC2 instances inside an Auto Scaling Group. The Auto Scaling group is configured to scale when CPU utilization of the instances is greater than 70%. The Auto Scaling group sits behind an Elastic Load Balancer, and your static content lives in S3 and is distributed globally by CloudFront. Your RDS database is an db.r3.8xlarge instance. Cloudwatch metrics show that your RDS instance usually has around 2GB of memory free, and an average CPU utilization of 75%. Currently, it is taking your users in Japan and Australia approximately 3 - 5 seconds to load your website, and you have been asked to help reduce these load-times. How might you improve your page load times? (Choose 3)

Set up a clone of your production environment in the Asia Pacific region and configure latency based routing on Route53.

Setup CloudFront with dynamic content support to enable the caching of re-usable content from the media rich website.

Change your Auto Scaling Group so that it will scale when CPU Utilization is only 50%, rather than 70%.

Use ElastiCache to cache the most commonly accessed DB queries.

Upgrade the RDS instance to a higher memory instance.

A,B,C

Your RDS instance is already the largest currently offered by AWS so you cannot upgrade this further. Changing your autoscaling policies will not help improve performance times as it is much more likely that the performance issue is with the database back end rather than the front end.

The risk with spot instances is that you are not guaranteed use of the resource for as long as you might want. Which of the following are scenarios under which AWS might execute a forced shutdown? (Choose 4)

AWS sends a notification of termination and you receive it 120 seconds before the intended forced shutdown, but AWS do not action the shutdown.

AWS sends a notification of termination and you receive it 120 seconds before the forced shutdown, and you delay it by sending a 'Delay300' instruction before the forced shutdown takes effect.

AWS sends a notification of termination and you receive it 120 seconds before the intended forced shutdown.

AWS sends a notification of termination and you receive it 120 seconds before the forced shutdown, but you block the shutdown because you used 'Termination Protection' when you initialized the instance.

AWS sends a notification of termination but you do not receive it within the 120 seconds and the instance is shutdown.

AWS sends a notification of termination and you receive it 120 seconds before the forced shutdown, but the normal lease expired before the forced shutdown.

ACEF

You are reviewing Change Control requests, and you note that there is a change designed to reduce costs by updating the "WaitTimeSeconds" attribute. What does this mean?

When the consumer instance polls for new work, the SQS service will allow it to wait a certain time for one or more messages to be available before closing the connection.

When the consumer instance polls for new work, the consumer instance will wait a certain time until it has a full workload before closing the connection.

While processing a message, a consumer instance can reset the message visibility by restarting the preset timeout counter.

While processing a message, a consumer instance can amend the message visibility counter by a fixed amount.

When a new message is added to the SQS queue, it will be hidden from consumer instances for a fixed period.

When a consumer instance retrieves a message, that message will be hidden in the queue for a fixed period.

When the consumer instance polls for new work, the SQS service will allow it to wait a certain time for one or more messages to be available before closing the connection.

You are reviewing Change Control requests and you note that there is a proposed change designed to reduce errors due to S3 Eventual Consistency by updating the "DelaySeconds" attribute. What does this mean?

When a consumer instance retrieves a message, that message will be hidden in the queue for a fixed period.

When the consumer instance polls for new work, the SQS service will allow it to wait a certain time for a message to be available before closing the connection.

While processing a message, a consumer instance can amend the message visibility counter by a fixed amount.

While processing a message, a consumer instance can reset the message visibility by restarting the preset timeout counter.

When the consumer instance polls for new work, the consumer instance will wait a certain time until it has a full workload before closing the connection.

When a new message is added to the SQS queue, it will be hidden from consumer instances for a fixed period.

When a new message is added to the SQS queue, it will be hidden from consumer instances for a fixed period.

You work for a popular media outlet about to release a story that is expected to go viral. During load testing on the website, you discover that there is read contention on the database tier of your application. Your RDS instance consists of a MySQL database on an extra large instance. Which of the following approaches would be best to further scale this instance to meet the anticipated increase in traffic your viral story will generate? (Choose 3)
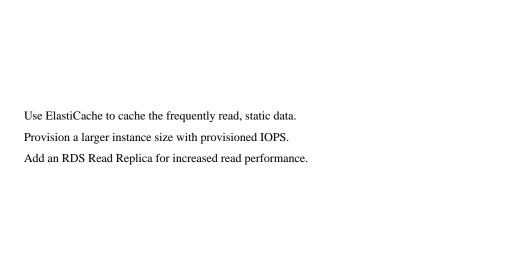
Add an RDS Read Replica for increased read performance.

Add an RDS Multi-AZ for increased read performance.

Use ElastiCache to cache the frequently read, static data.

Provision a larger instance size with provisioned IOPS.

Shard the MySQL database into multiple copies.

Use ElastiCache to cache the frequently read, static data.

Provision a larger instance size with provisioned IOPS.

Add an RDS Read Replica for increased read performance.

To add an object to an S3 bucket, the PUT operation is used. As part of crafting a PUT, the programmer can add instructions called Request Headers. Which of the following are valid S3 Request Headers? (Choose 4)

x-aws-storage-class

x-amz-meta-

Content-Length

x-amz-storage-class

Content-MD5

x-aws-meta-

Cache-Enable

x-amz-meta-

Content-Length

x-amz-storage-class

Content-MD5

You are a solutions architect with a manufacturing company running several legacy applications. One of these applications needs to communicate with services which are currently hosted on-premise. The people who wrote this application have left the company, and there is no documentation describing how the application works. You need to ensure that this application can be hosted in a bespoke VPC, but remains able to communicate to the back-end services hosted on-premise. Which of the following answers will allow the application to communicate back to the on premise equipment without the need to reprogram the application? (Choose 3)

You should configure an AWS Direct Connect link between the VPC and the site with the on-premise solution.

You should attach an Elastic IP address to the VPC so that it will be able to communicate with the on-premise site.

You should configure your Elastic Load Balancer to act as a reverse proxy so that the EC2 instance can communicate back to the on-premise data center.

You should configure the VPC subnet in which the application sits so that it does not have an IP address range that conflicts with that of the on-premise VLAN in which the back end services sit.

You should ensure the VPC has an internet gateway attached to it. That way, you can establish a site-to-site VPN with the on-premise environment.

1,4,5

You are a solutions architect working for an oil and gas company. They are moving their production environment to AWS and need a custom VPC into which to put it. You have been asked to create a public subnet. You create the VPC with a subnet bearing the CIDR address range of 10.0.1.0/24. Which of the following steps should you take to make this subnet public? (Choose 2)

Attach an Internet Gateway (IGW) to the VPC.

Attach a Customer Gateway (CGW).

Create a route in the route table of the subnet allowing a route out of the Internet Gateway (IGW).

In the AWS console, right click on the subnet and then select the Make Public option.

Create a route in the route table of the subnet allowing a route out of the Customer Gateway (CGW).

1,3