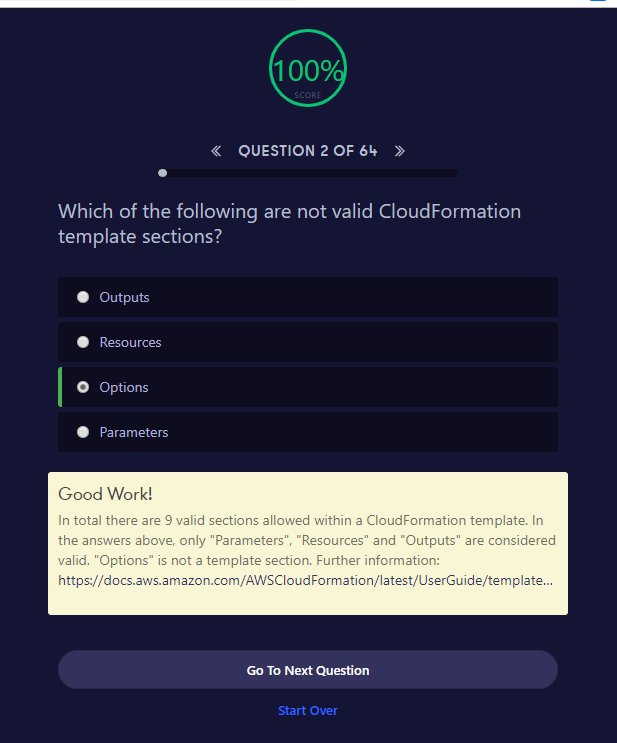


Good Work!

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>



##### Good Work!

In total there are 9 valid sections allowed within a CloudFormation template. In the answers above, only "Parameters", "Resources" and "Outputs" are considered valid. "Options" is not a template section. Further information: <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html>

{

"AWSTemplateFormatVersion" : "*version date*",

"Description" : "*JSON string*",

"Metadata" : {

*template metadata*

},

"Parameters" : {

*set of parameters*

},

"Mappings" : {

*set of mappings*

},

"Conditions" : {

*set of conditions*

},

"Transform" : {

*set of transforms*

},

"Resources" : {

*set of resources*

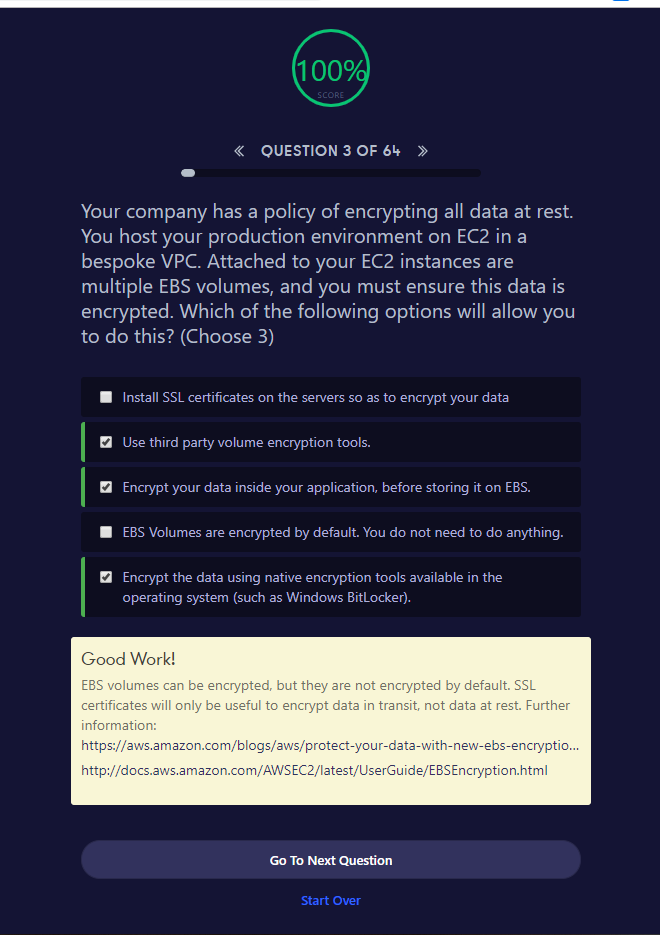
},

"Outputs" : {

*set of outputs*

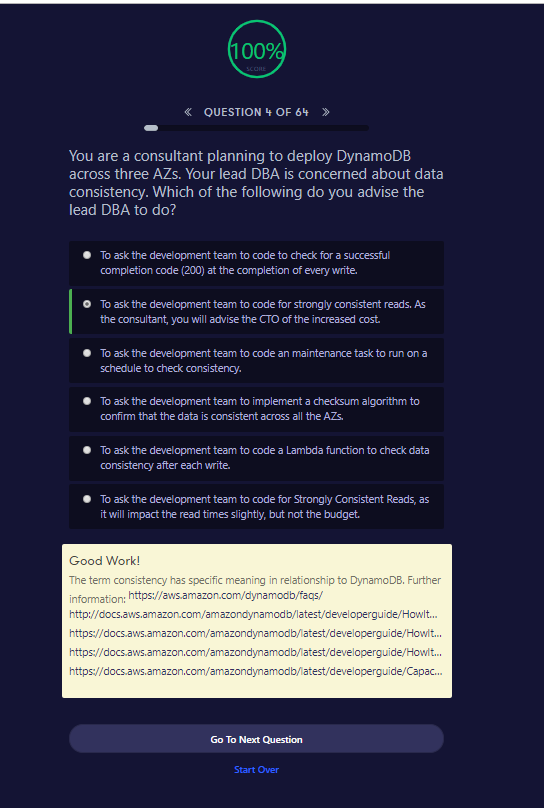
}

}



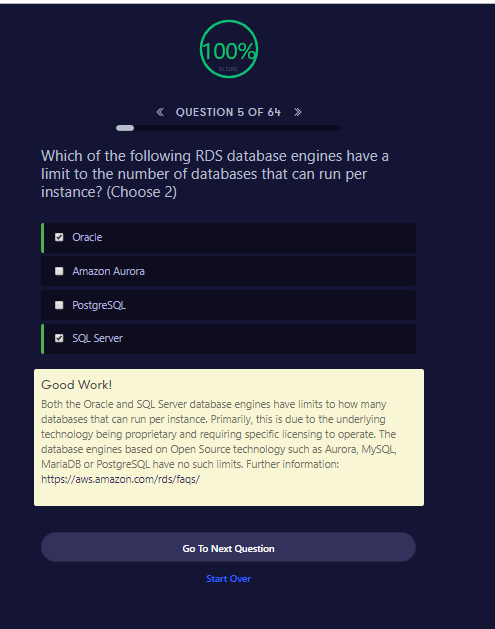
##### Good Work!

EBS volumes can be encrypted, but they are not encrypted by default. SSL certificates will only be useful to encrypt data in transit, not data at rest. Further information: <https://aws.amazon.com/blogs/aws/protect-your-data-with-new-ebs-encryption/><http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>



##### Good Work!

The term consistency has specific meaning in relationship to DynamoDB. Further information: <https://aws.amazon.com/dynamodb/faqs/><http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.DataConsistency.html><https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadConsistency.html><https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ProvisionedThroughput.html><https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/CapacityUnitCalculations.html>

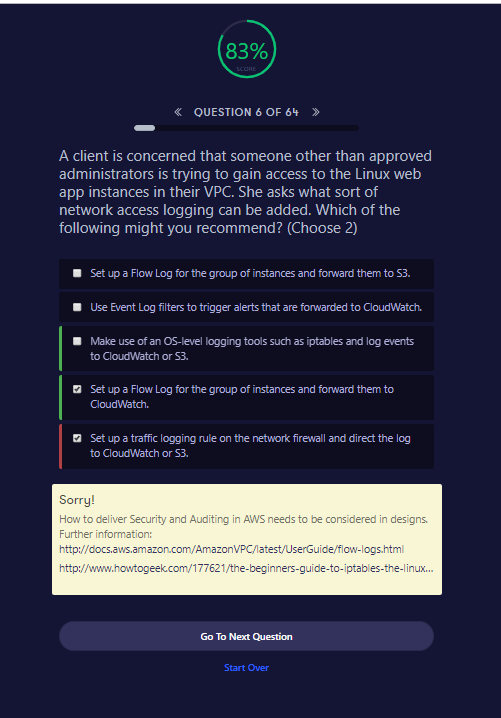


##### Good Work!

Both the Oracle and SQL Server database engines have limits to how many databases that can run per instance. Primarily, this is due to the underlying technology being proprietary and requiring specific licensing to operate. The database engines based on Open Source technology such as Aurora, MySQL, MariaDB or PostgreSQL have no such limits. Further information: <https://aws.amazon.com/rds/faqs/>

By default, customers are allowed to **have** up to a total of 40 Amazon **RDS DB instances**. Of those 40, up to 10 **can** be Oracle or SQL Server **DB Instances** under the "License Included" model. All 40 **can** be used for MySQL, Oracle, SQL Server, or PostgreSQL under the "BYOL" model.

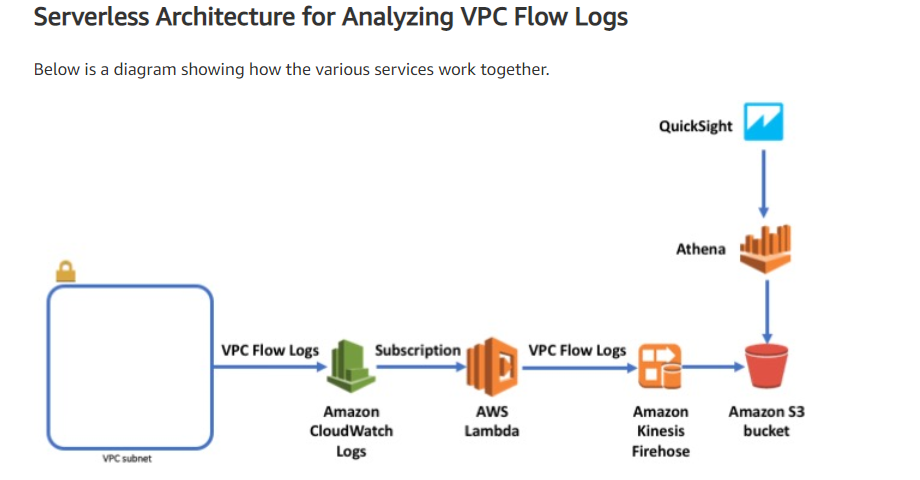
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Limits.html>

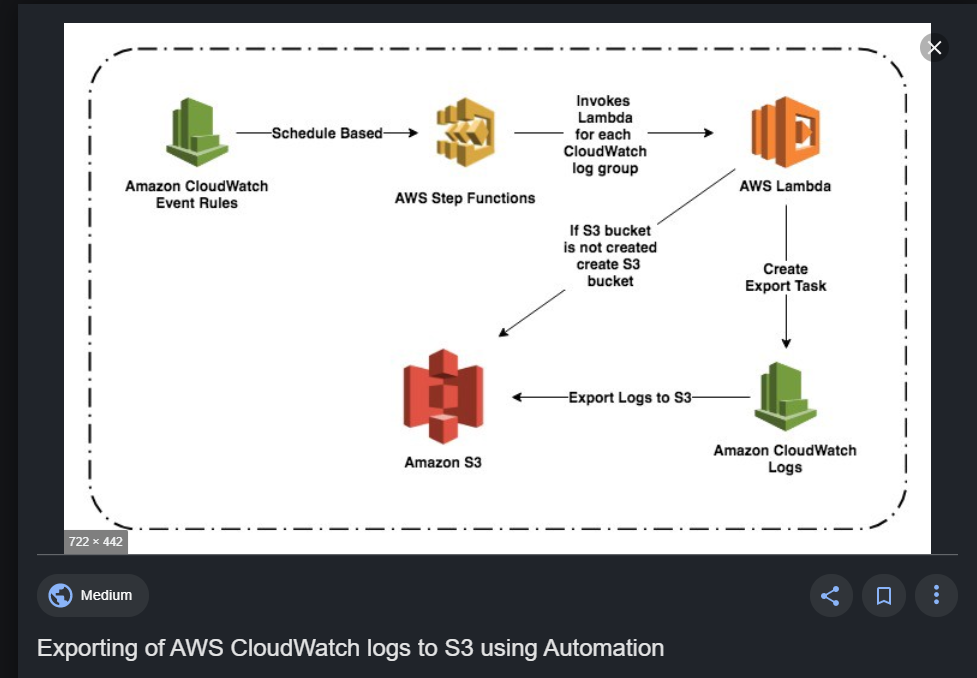


##### Sorry!

How to deliver Security and Auditing in AWS needs to be considered in designs. Further information: <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html><http://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/>

<https://aws.amazon.com/blogs/big-data/analyzing-vpc-flow-logs-with-amazon-kinesis-firehose-amazon-athena-and-amazon-quicksight/>

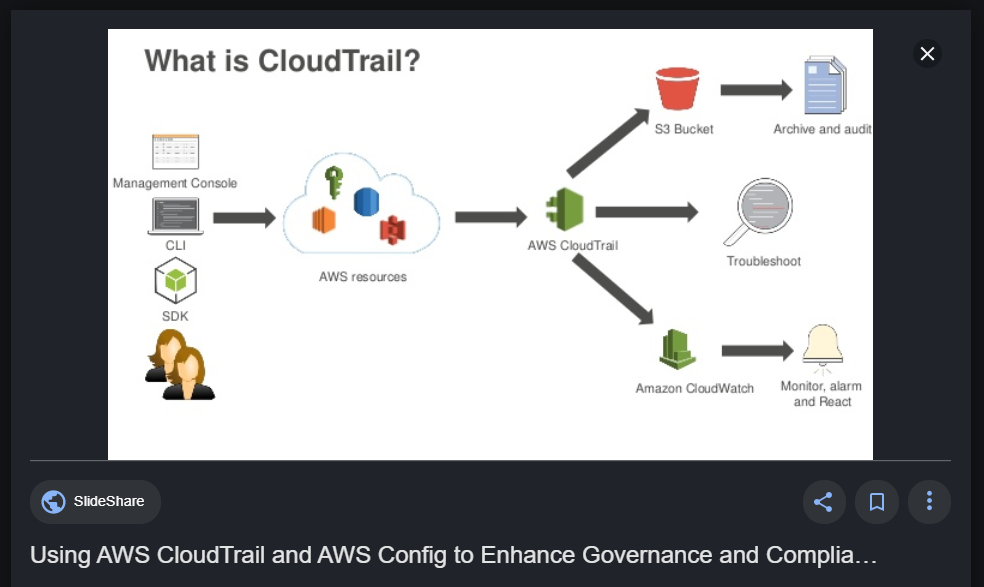


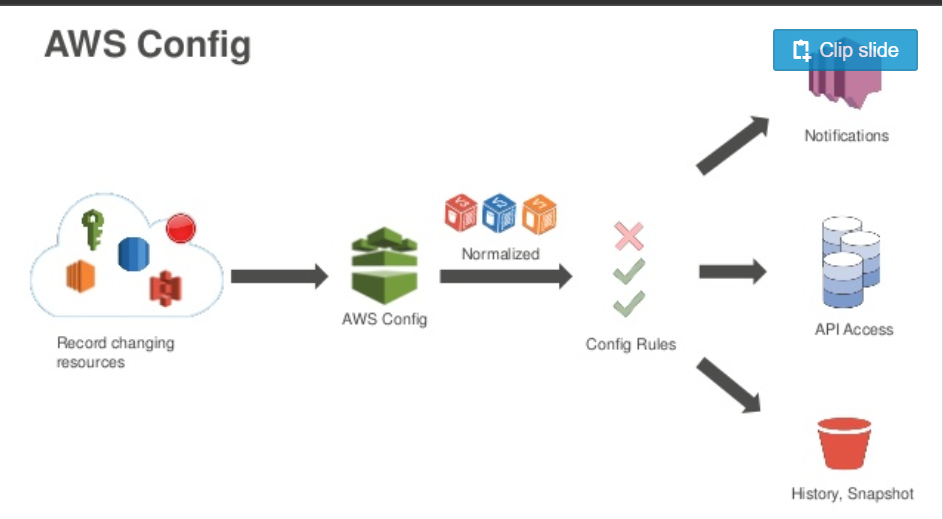




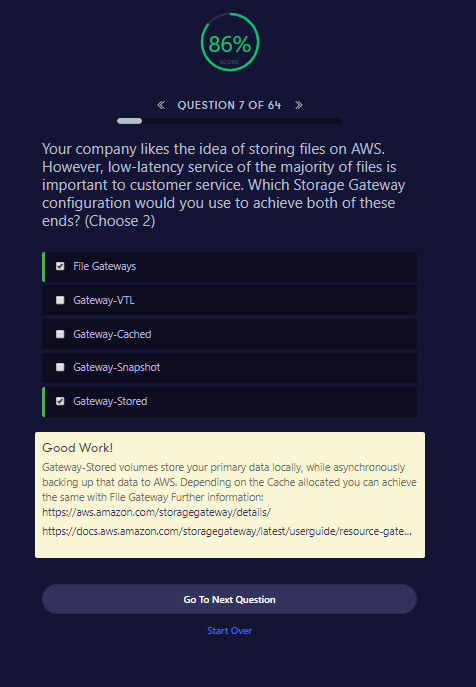
Cloud Trail, Cloud Watch and AWS Config

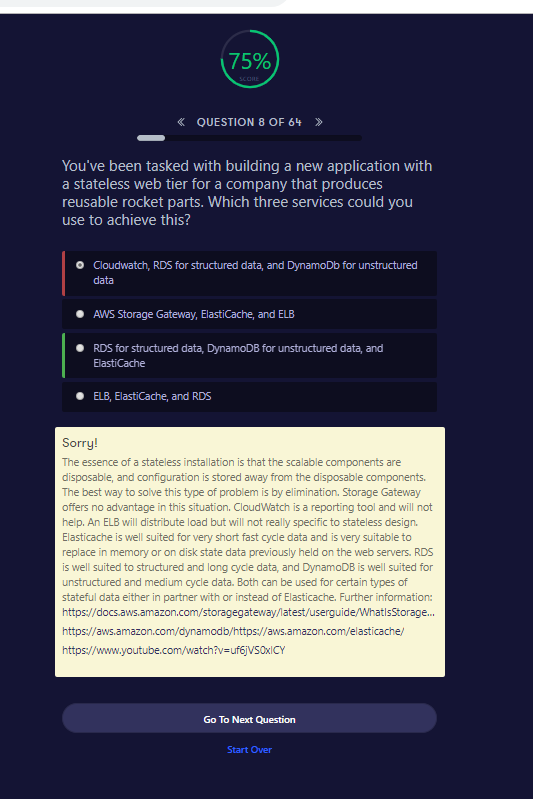
<https://www.slideshare.net/AmazonWebServices/using-aws-cloudtrail-and-aws-config-to-enhance-governance-and-compliance-of-amazon-s3>



. 

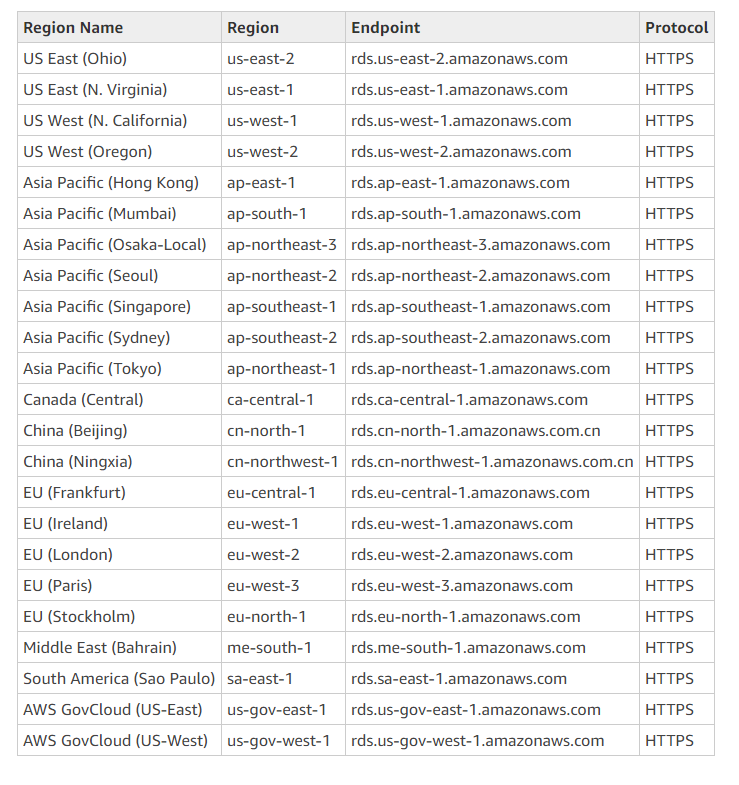


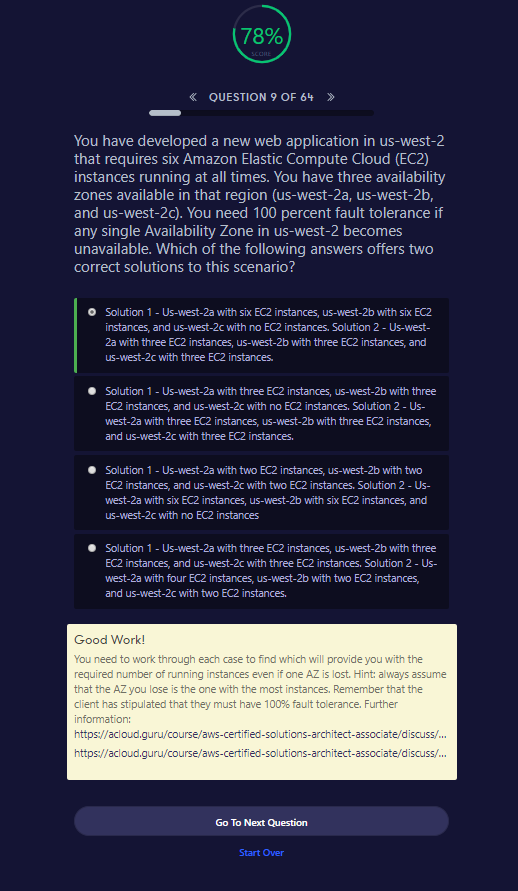


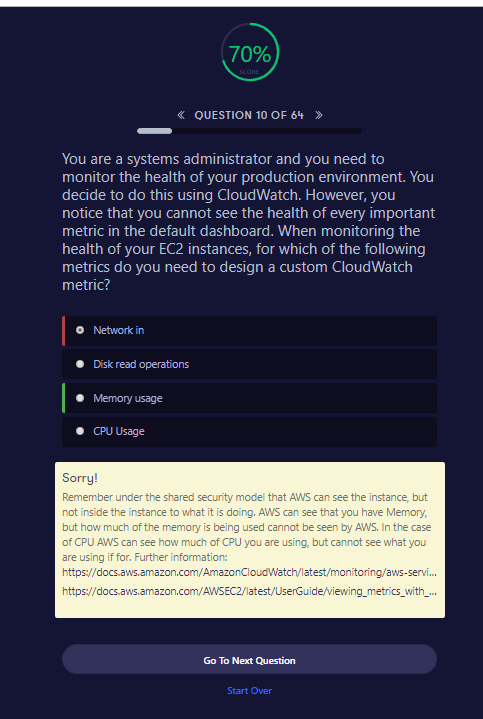


##### Sorry!

The essence of a stateless installation is that the scalable components are disposable, and configuration is stored away from the disposable components. The best way to solve this type of problem is by elimination. Storage Gateway offers no advantage in this situation. CloudWatch is a reporting tool and will not help. An ELB will distribute load but will not really specific to stateless design. Elasticache is well suited for very short fast cycle data and is very suitable to replace in memory or on disk state data previously held on the web servers. RDS is well suited to structured and long cycle data, and DynamoDB is well suited for unstructured and medium cycle data. Both can be used for certain types of stateful data either in partner with or instead of Elasticache. Further information: <https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html><https://aws.amazon.com/dynamodb/><https://aws.amazon.com/elasticache/><https://www.youtube.com/watch?v=uf6jVS0xlCY>

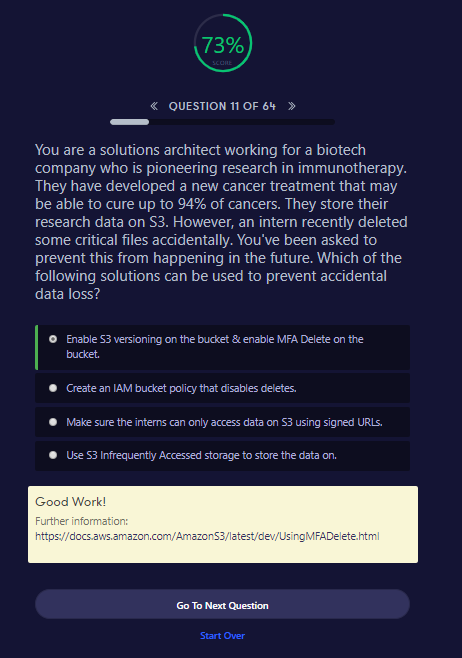


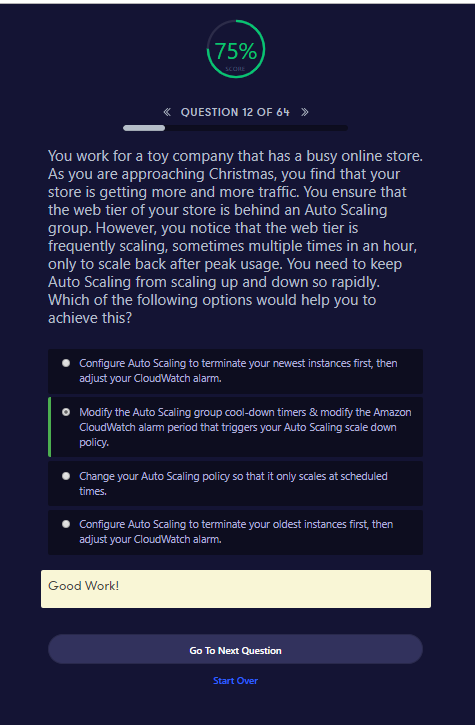


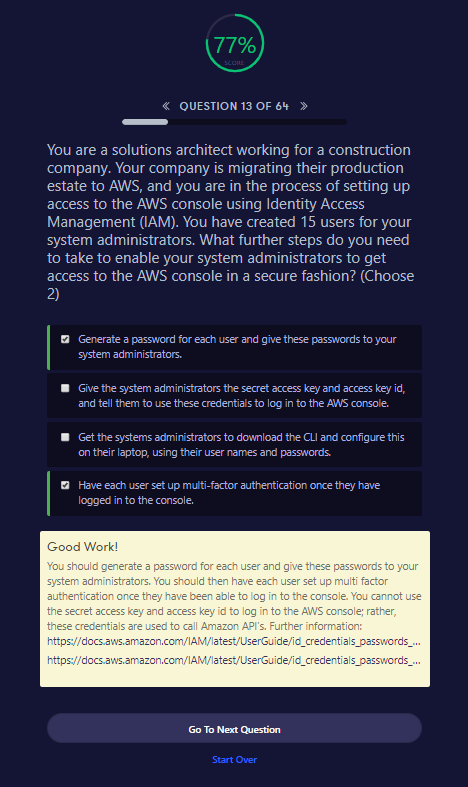


##### Sorry!

Remember under the shared security model that AWS can see the instance, but not inside the instance to what it is doing. AWS can see that you have Memory, but how much of the memory is being used cannot be seen by AWS. In the case of CPU AWS can see how much of CPU you are using, but cannot see what you are using if for. Further information: <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-services-cloudwatch-metrics.html><https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html>

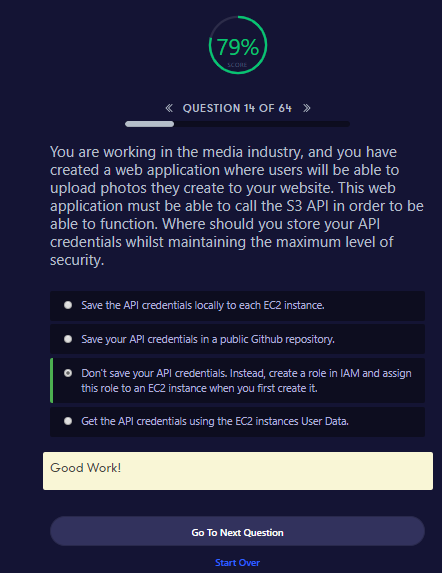


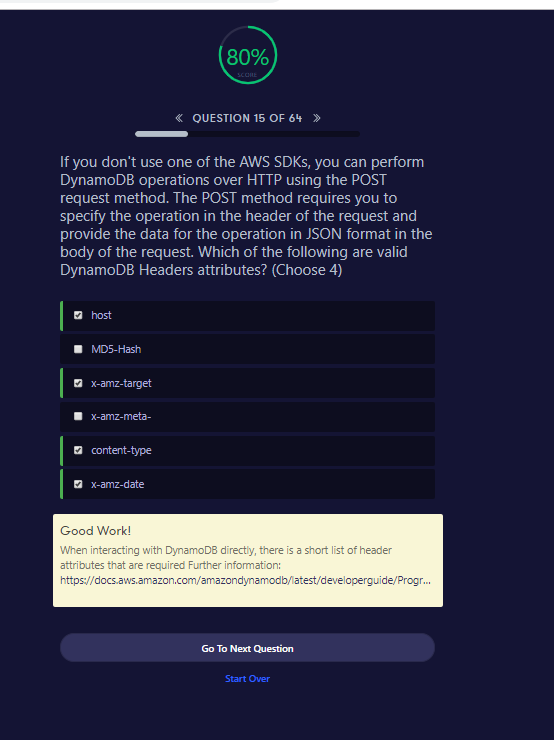


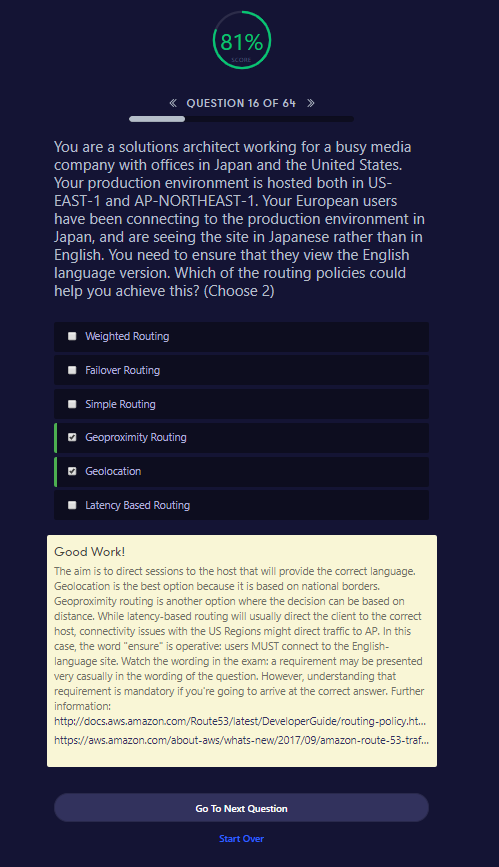


##### Good Work!

You should generate a password for each user and give these passwords to your system administrators. You should then have each user set up multi factor authentication once they have been able to log in to the console. You cannot use the secret access key and access key id to log in to the AWS console; rather, these credentials are used to call Amazon API’s. Further information: <https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_admin-change-user.html><https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_user-change-own.html>

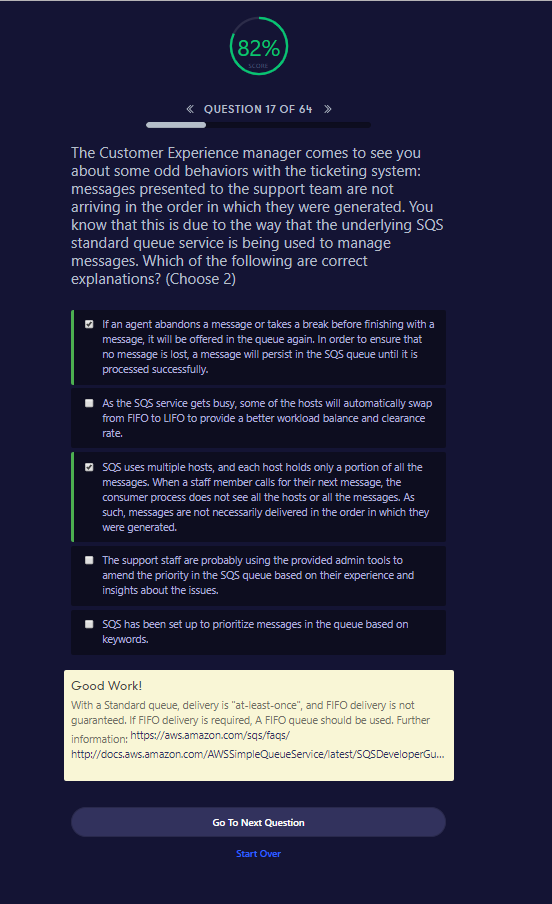






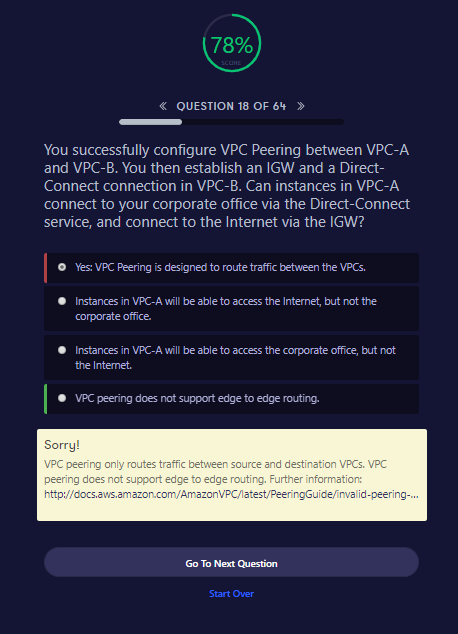
##### Good Work!

The aim is to direct sessions to the host that will provide the correct language. Geolocation is the best option because it is based on national borders. Geoproximity routing is another option where the decision can be based on distance. While latency-based routing will usually direct the client to the correct host, connectivity issues with the US Regions might direct traffic to AP. In this case, the word "ensure" is operative: users MUST connect to the English-language site. Watch the wording in the exam: a requirement may be presented very casually in the wording of the question. However, understanding that requirement is mandatory if you're going to arrive at the correct answer. Further information: <http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html><https://aws.amazon.com/about-aws/whats-new/2017/09/amazon-route-53-traffic-flow-announces-support-for-geoproximity-routing-with-traffic-biasing/>



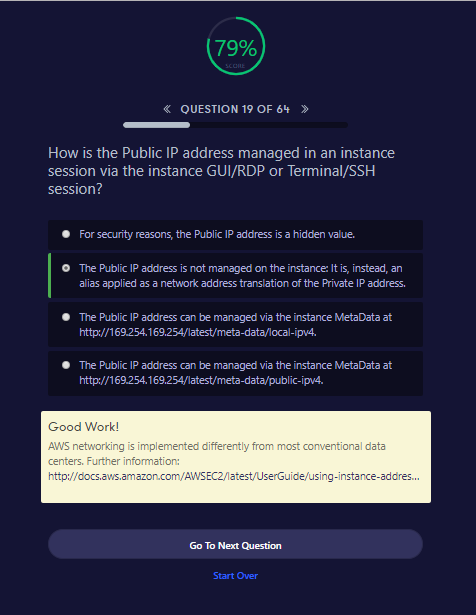
##### Good Work!

With a Standard queue, delivery is "at-least-once", and FIFO delivery is not guaranteed. If FIFO delivery is required, A FIFO queue should be used. Further information: <https://aws.amazon.com/sqs/faqs/><http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/DistributedQueues.html>



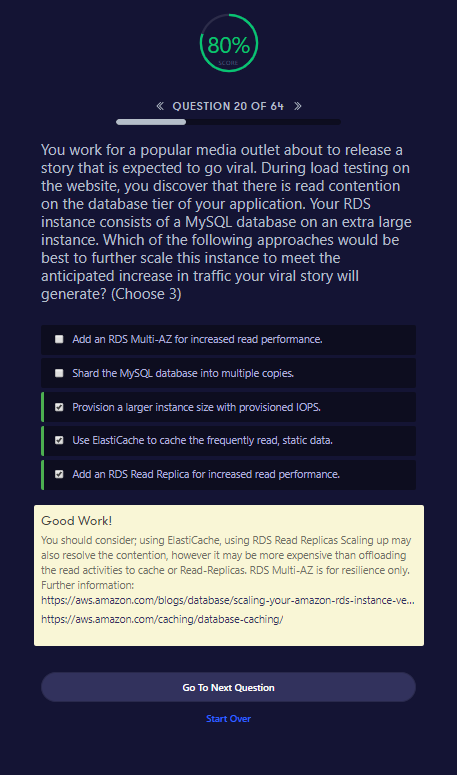
##### Sorry!

VPC peering only routes traffic between source and destination VPCs. VPC peering does not support edge to edge routing. Further information: <http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/invalid-peering-configurations.html>



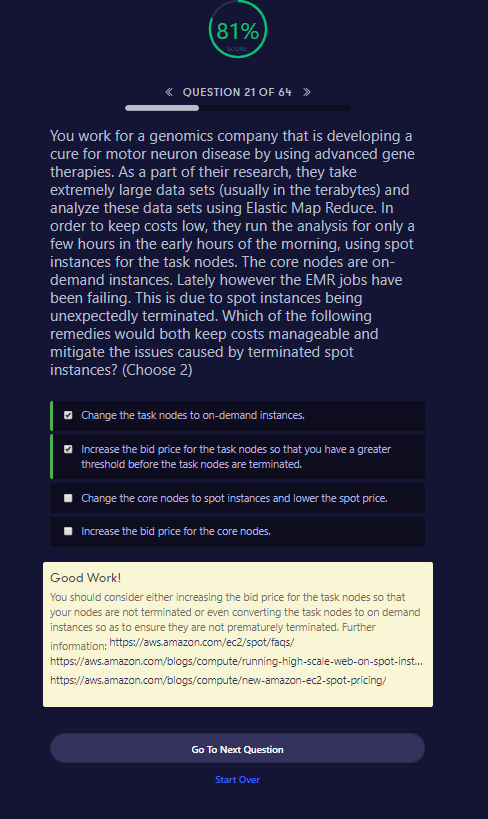
##### Good Work!

AWS networking is implemented differently from most conventional data centers. Further information: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>



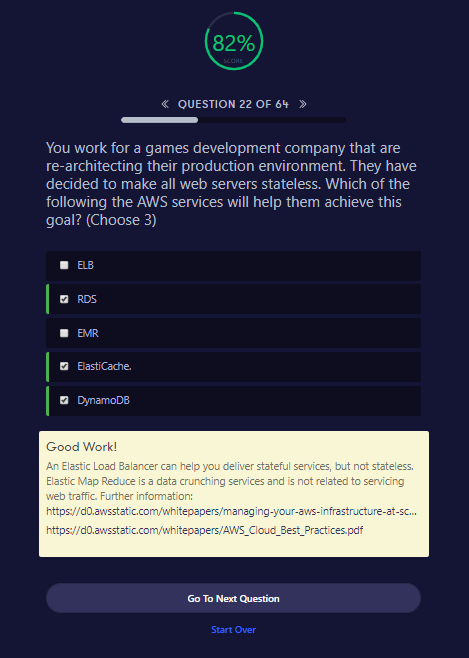
##### Good Work!

You should consider; using ElastiCache, using RDS Read Replicas Scaling up may also resolve the contention, however it may be more expensive than offloading the read activities to cache or Read-Replicas. RDS Multi-AZ is for resilience only. Further information: <https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/><https://aws.amazon.com/caching/database-caching/>



##### Good Work!

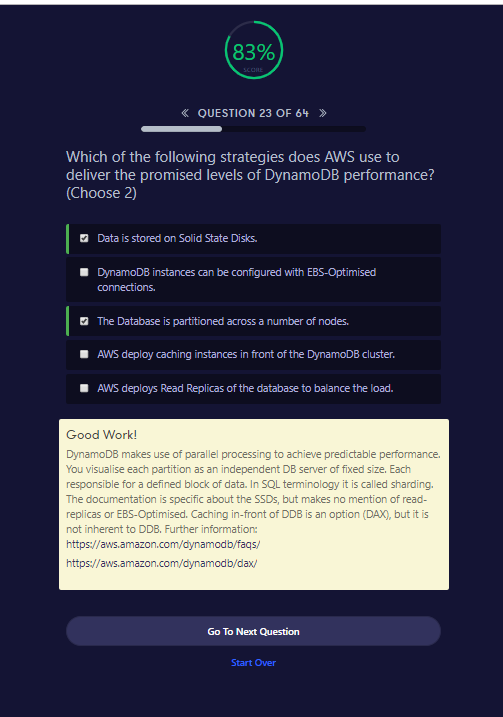
You should consider either increasing the bid price for the task nodes so that your nodes are not terminated or even converting the task nodes to on demand instances so as to ensure they are not prematurely terminated. Further information: <https://aws.amazon.com/ec2/spot/faqs/><https://aws.amazon.com/blogs/compute/running-high-scale-web-on-spot-instances/><https://aws.amazon.com/blogs/compute/new-amazon-ec2-spot-pricing/>



Good Work!

An Elastic Load Balancer can help you deliver stateful services, but not stateless. Elastic Map Reduce is a data crunching services and is not related to servicing web traffic. Further information: <https://d0.awsstatic.com/whitepapers/managing-your-aws-infrastructure-at-scale.pdf><https://d0.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf>

Go To Next QuestionStart Over



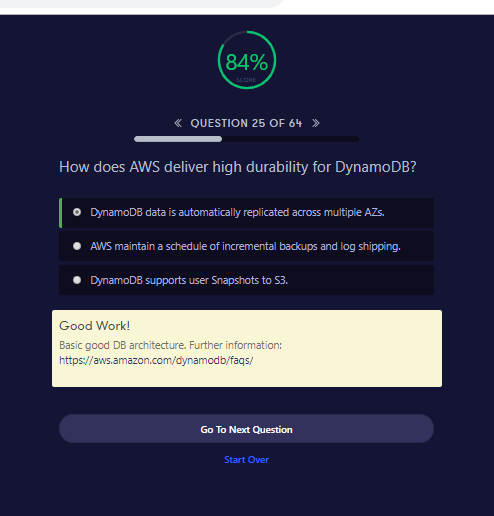
##### Good Work!

DynamoDB makes use of parallel processing to achieve predictable performance. You visualise each partition as an independent DB server of fixed size. Each responsible for a defined block of data. In SQL terminology it is called sharding. The documentation is specific about the SSDs, but makes no mention of read-replicas or EBS-Optimised. Caching in-front of DDB is an option (DAX), but it is not inherent to DDB. Further information: <https://aws.amazon.com/dynamodb/faqs/><https://aws.amazon.com/dynamodb/dax/>



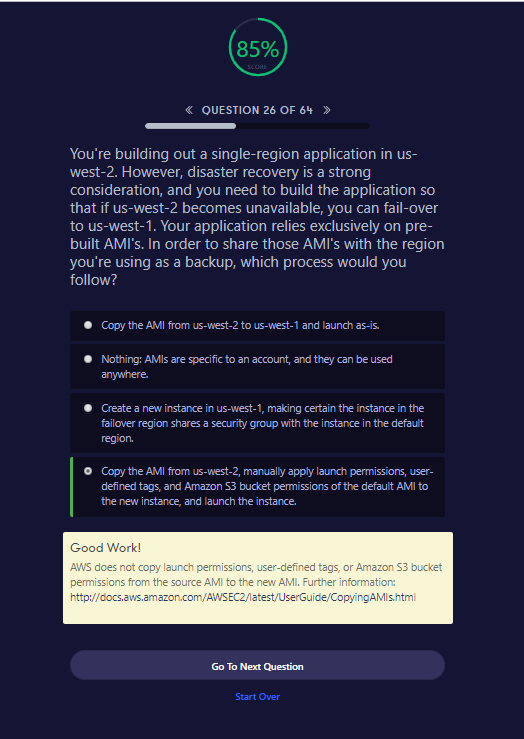
##### Good Work!

There are many features which are native to the KMS service. However, of the above, only import your own keys, disable and re-enable keys and define key management roles in IAM are valid. Importing keys into a custom key store and migrating keys from the default key store to a custom key store are not possible. Lastly operating as a private, native HSM is a function of CloudHSM and is not possible directly within KMS. Further information: <https://aws.amazon.com/kms/faqs/>



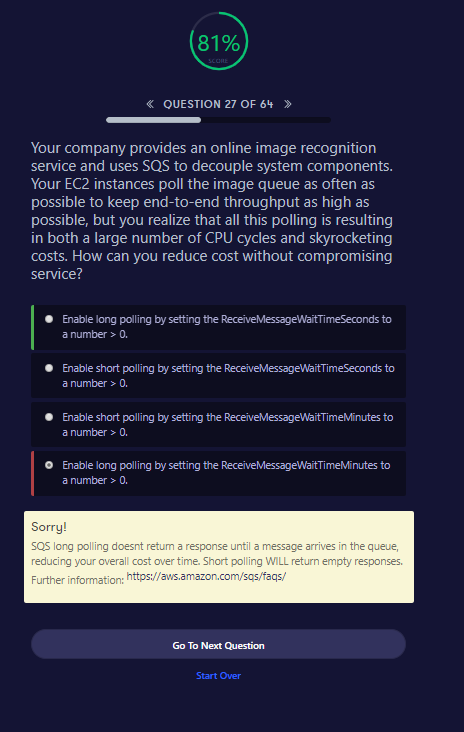
##### Good Work!

Basic good DB architecture. Further information: <https://aws.amazon.com/dynamodb/faqs/>



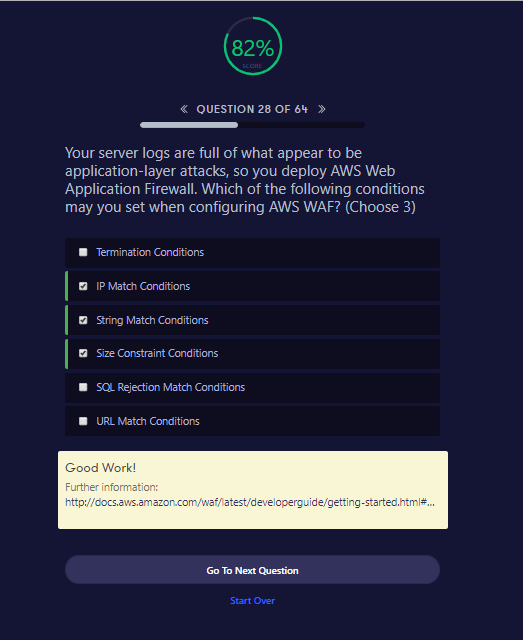
##### Good Work!

AWS does not copy launch permissions, user-defined tags, or Amazon S3 bucket permissions from the source AMI to the new AMI. Further information: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html>



##### Sorry!

SQS long polling doesnt return a response until a message arrives in the queue, reducing your overall cost over time. Short polling WILL return empty responses. Further information: <https://aws.amazon.com/sqs/faqs/>

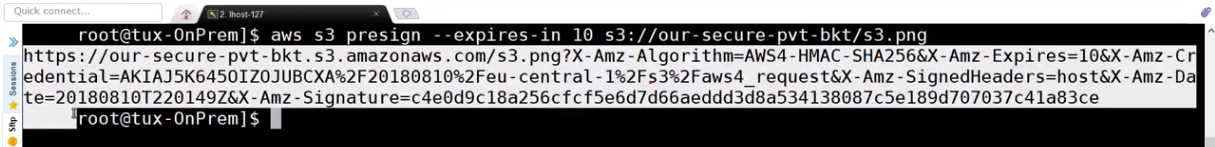


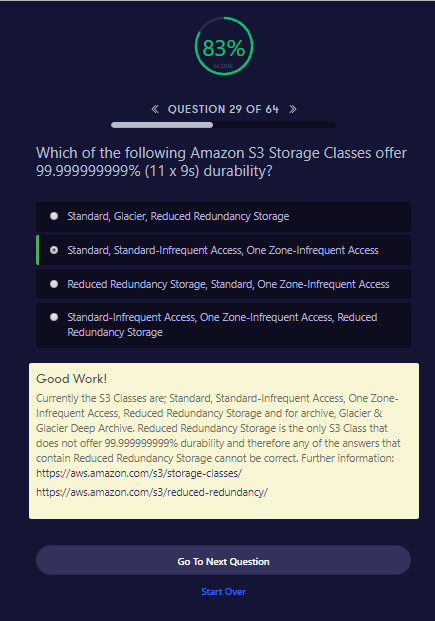
Good Work!

Further information: <http://docs.aws.amazon.com/waf/latest/developerguide/getting-started.html#getting-started-wizard-create-web-acl>

Go To Next QuestionStart Over

Read WAF conditions and Rules and Wb ACLs in detail to answer such questions

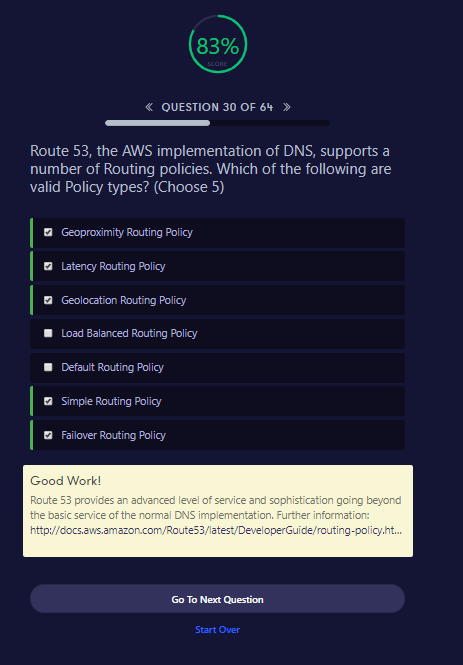






##### Good Work!

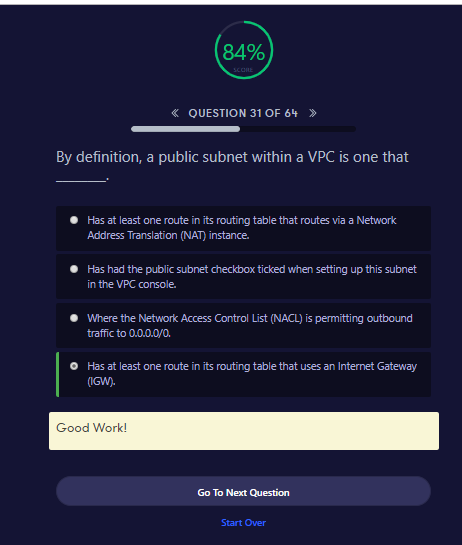
Currently the S3 Classes are; Standard, Standard-Infrequent Access, One Zone-Infrequent Access, Reduced Redundancy Storage and for archive, Glacier & Glacier Deep Archive. Reduced Redundancy Storage is the only S3 Class that does not offer 99.999999999% durability and therefore any of the answers that contain Reduced Redundancy Storage cannot be correct. Further information: <https://aws.amazon.com/s3/storage-classes/><https://aws.amazon.com/s3/reduced-redundancy/>

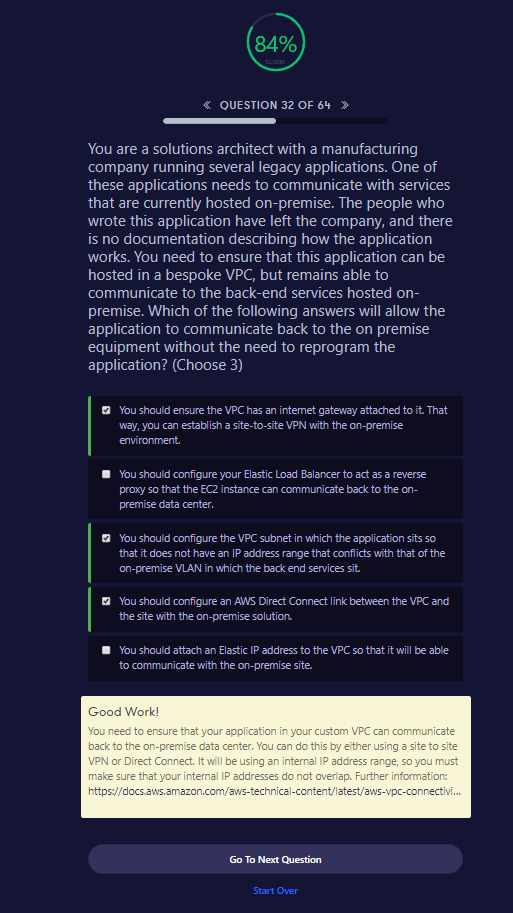


Good Work!

Route 53 provides an advanced level of service and sophistication going beyond the basic service of the normal DNS implementation. Further information: <http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

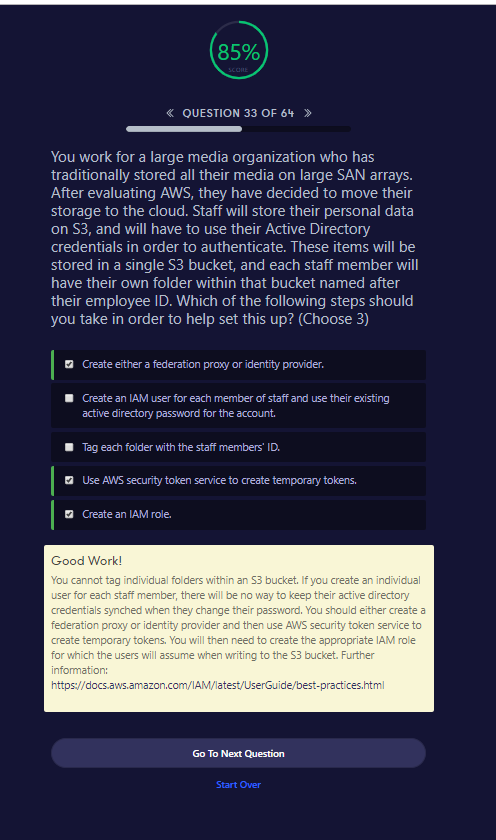
Go To Next QuestionStart Over





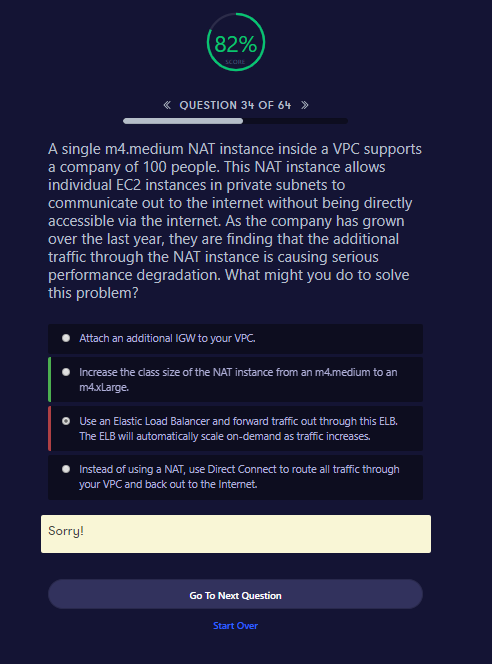
##### Good Work!

You need to ensure that your application in your custom VPC can communicate back to the on-premise data center. You can do this by either using a site to site VPN or Direct Connect. It will be using an internal IP address range, so you must make sure that your internal IP addresses do not overlap. Further information: <https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/network-to-amazon-vpc-connectivity-options.html>



##### Good Work!

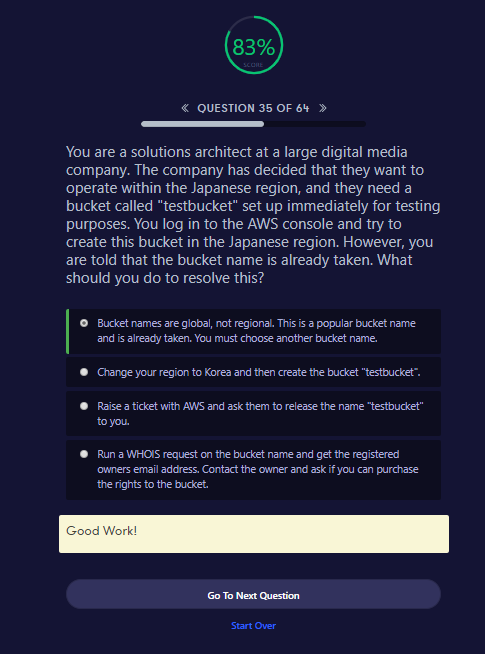
You cannot tag individual folders within an S3 bucket. If you create an individual user for each staff member, there will be no way to keep their active directory credentials synched when they change their password. You should either create a federation proxy or identity provider and then use AWS security token service to create temporary tokens. You will then need to create the appropriate IAM role for which the users will assume when writing to the S3 bucket. Further information: <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

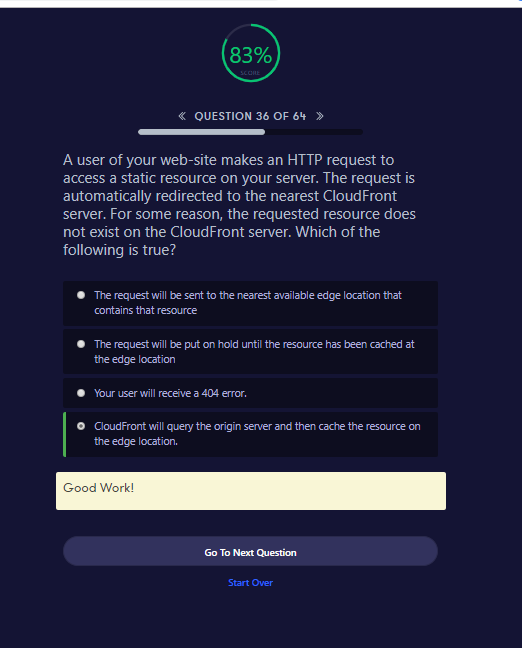


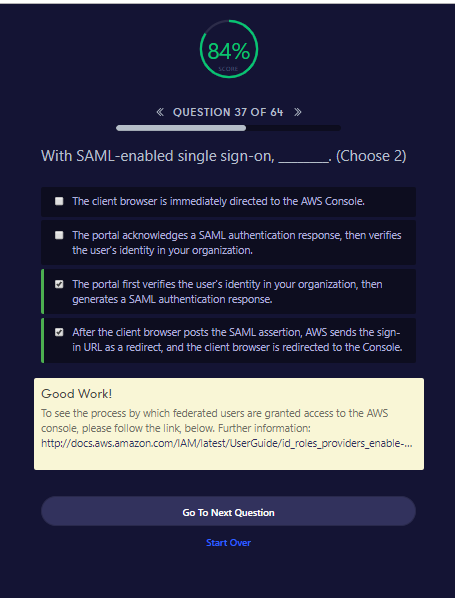
This is still questionable

<https://forums.aws.amazon.com/thread.jspa?threadID=92019>

<https://stackoverflow.com/questions/39037264/aws-elb-and-nat-gateway-not-playing-well-together>



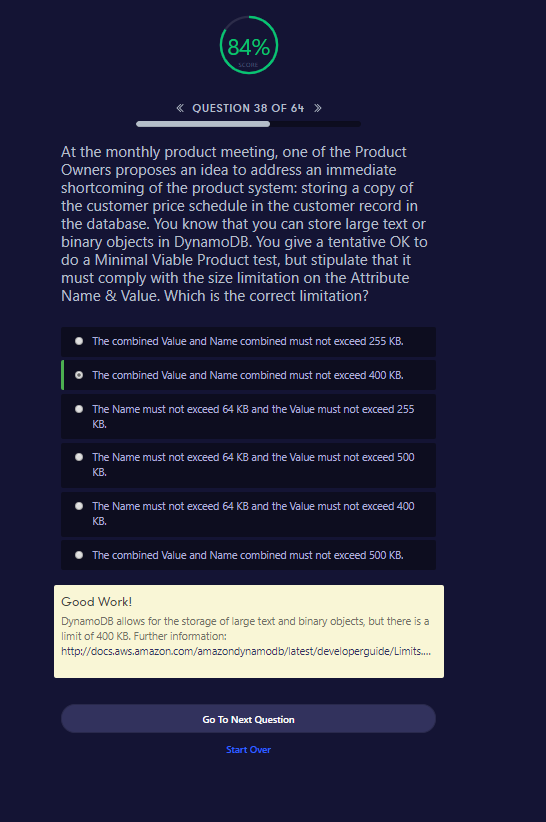




##### Good Work!

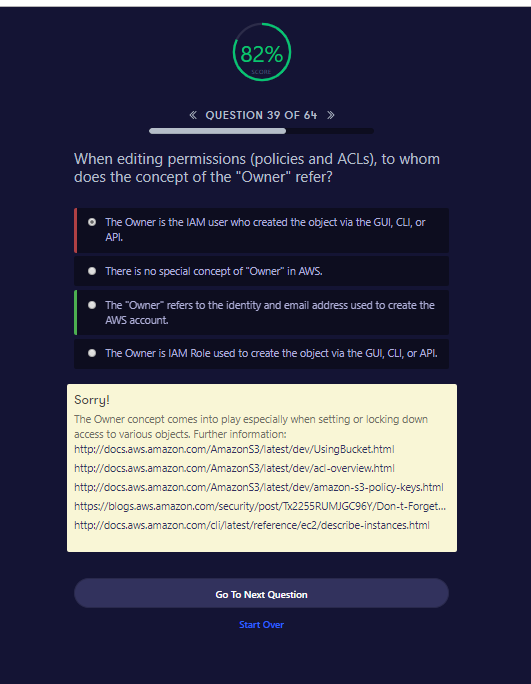
To see the process by which federated users are granted access to the AWS console, please follow the link, below. Further information: <http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html>

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html>



##### Good Work!

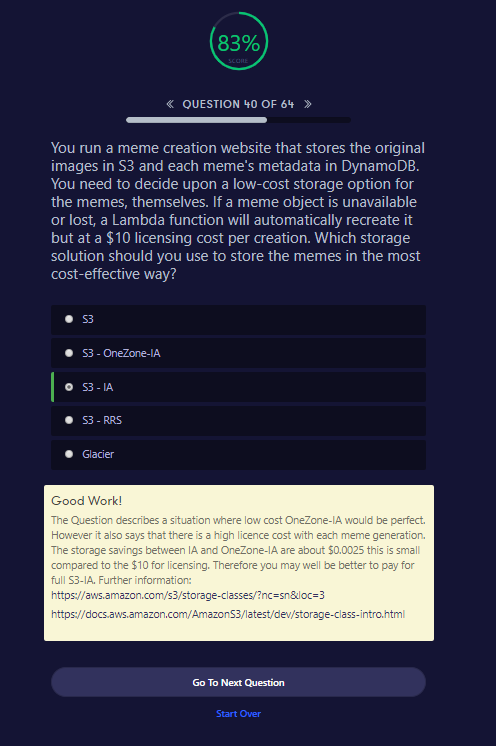
DynamoDB allows for the storage of large text and binary objects, but there is a limit of 400 KB. Further information: <http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Limits.html>



Sorry!

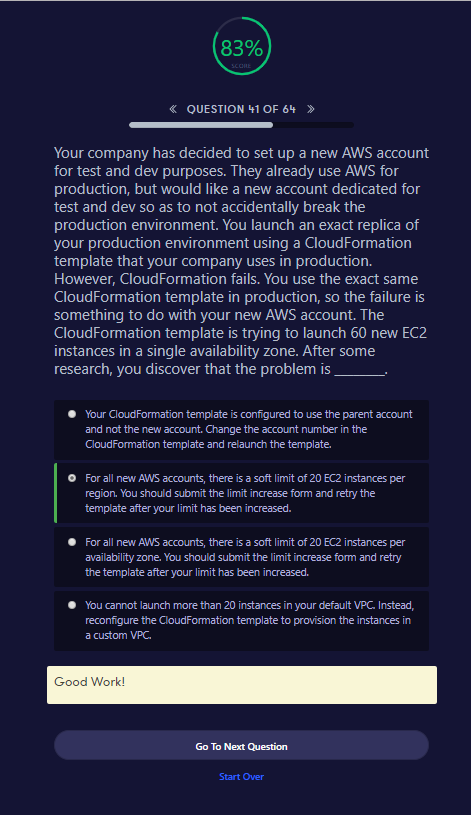
The Owner concept comes into play especially when setting or locking down access to various objects. Further information: <http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html><http://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html><http://docs.aws.amazon.com/AmazonS3/latest/dev/amazon-s3-policy-keys.html><https://blogs.aws.amazon.com/security/post/Tx2255RUMJGC96Y/Don-t-Forget-to-Enable-Access-to-the-Billing-Console><http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html>

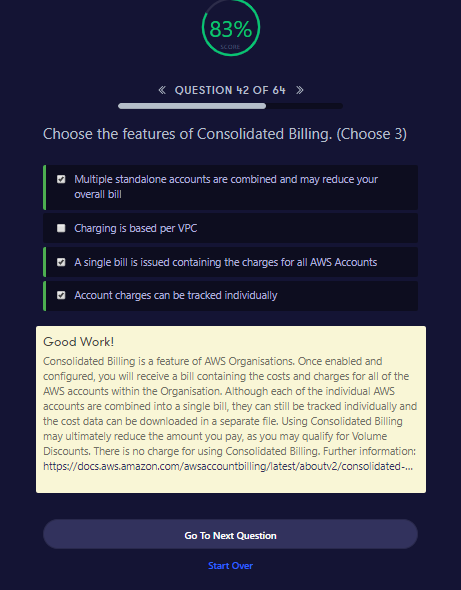
Go To Next QuestionStart Over



##### Good Work!

The Question describes a situation where low cost OneZone-IA would be perfect. However it also says that there is a high licence cost with each meme generation. The storage savings between IA and OneZone-IA are about $0.0025 this is small compared to the $10 for licensing. Therefore you may well be better to pay for full S3-IA. Further information: <https://aws.amazon.com/s3/storage-classes/?nc=sn&loc=3><https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html>

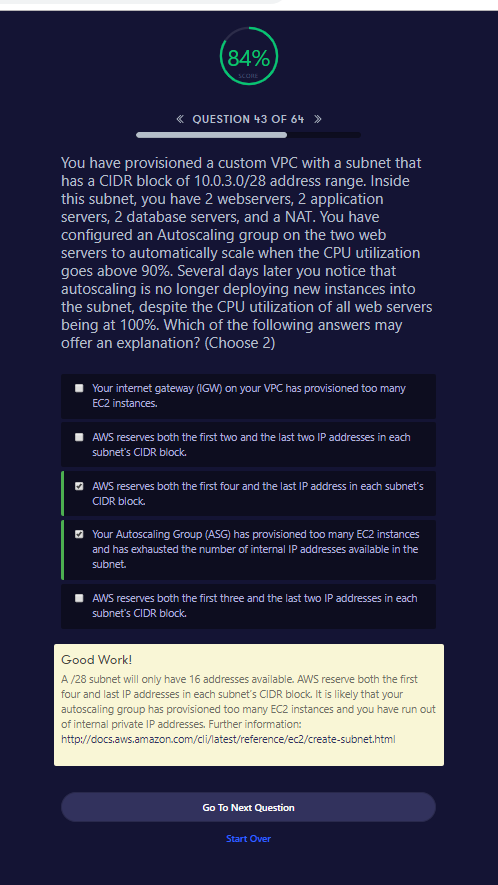




Good Work!

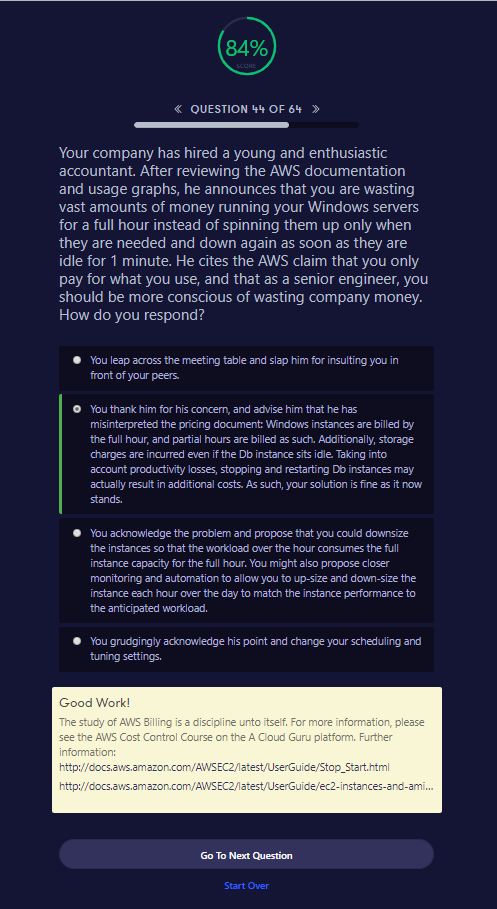
Consolidated Billing is a feature of AWS Organisations. Once enabled and configured, you will receive a bill containing the costs and charges for all of the AWS accounts within the Organisation. Although each of the individual AWS accounts are combined into a single bill, they can still be tracked individually and the cost data can be downloaded in a separate file. Using Consolidated Billing may ultimately reduce the amount you pay, as you may qualify for Volume Discounts. There is no charge for using Consolidated Billing. Further information: <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

Go To Next QuestionStart Over



##### Good Work!

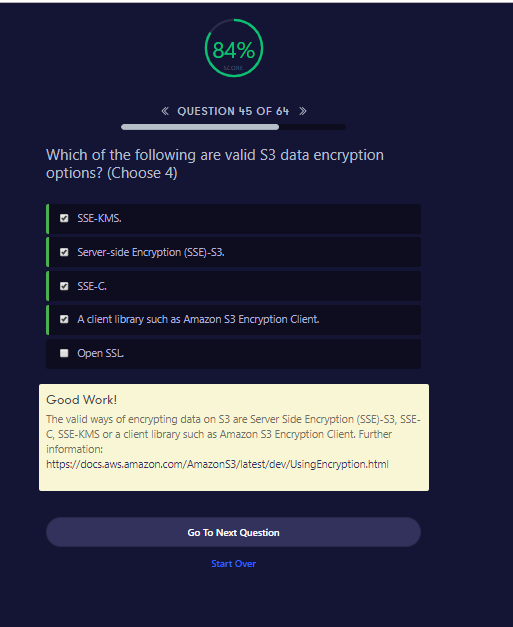
A /28 subnet will only have 16 addresses available. AWS reserve both the first four and last IP addresses in each subnet’s CIDR block. It is likely that your autoscaling group has provisioned too many EC2 instances and you have run out of internal private IP addresses. Further information: <http://docs.aws.amazon.com/cli/latest/reference/ec2/create-subnet.html>



Good Work!

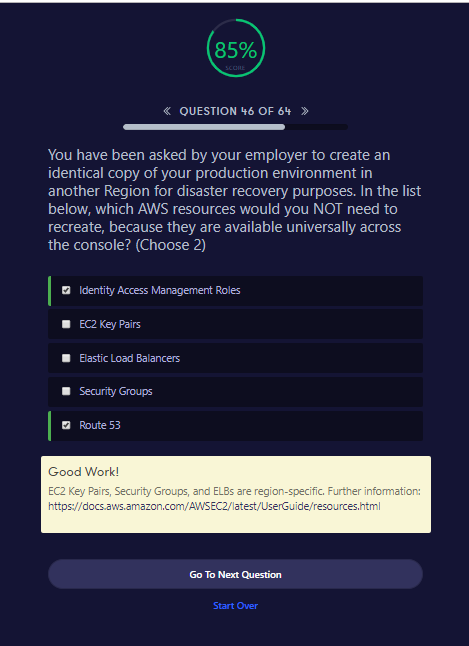
The study of AWS Billing is a discipline unto itself. For more information, please see the AWS Cost Control Course on the A Cloud Guru platform. Further information: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html><http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instances-and-amis.html>

Go To Next QuestionStart Over



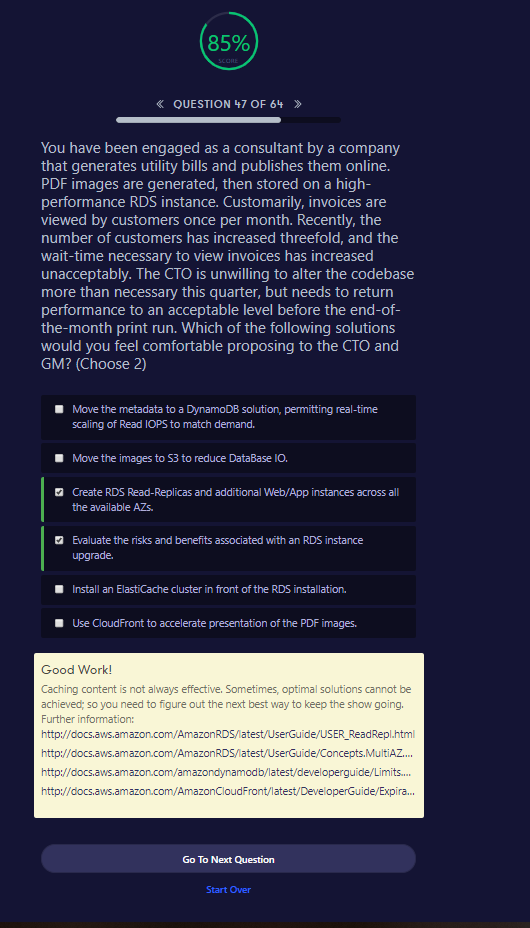
##### Good Work!

The valid ways of encrypting data on S3 are Server Side Encryption (SSE)-S3, SSE-C, SSE-KMS or a client library such as Amazon S3 Encryption Client. Further information: <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>



##### Good Work!

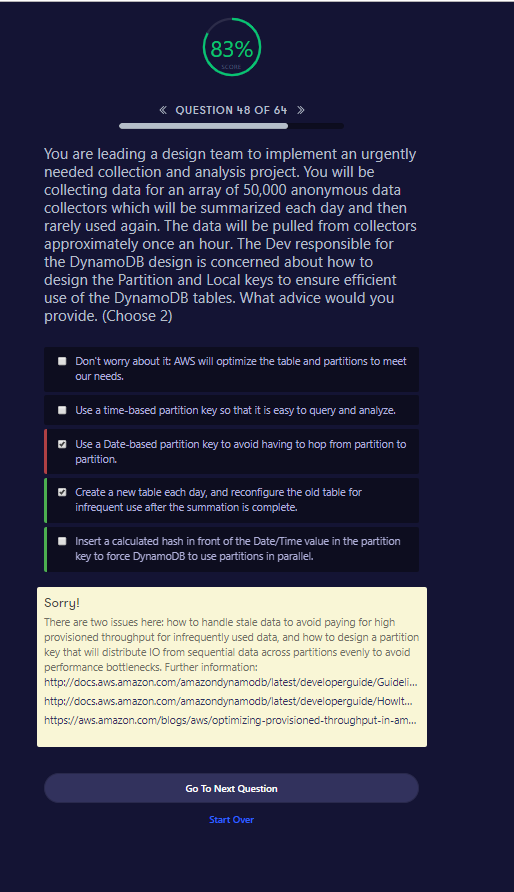
EC2 Key Pairs, Security Groups, and ELBs are region-specific. Further information: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html>



Good Work!

Caching content is not always effective. Sometimes, optimal solutions cannot be achieved; so you need to figure out the next best way to keep the show going. Further information: <http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html><http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html><http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Limits.html><http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html>

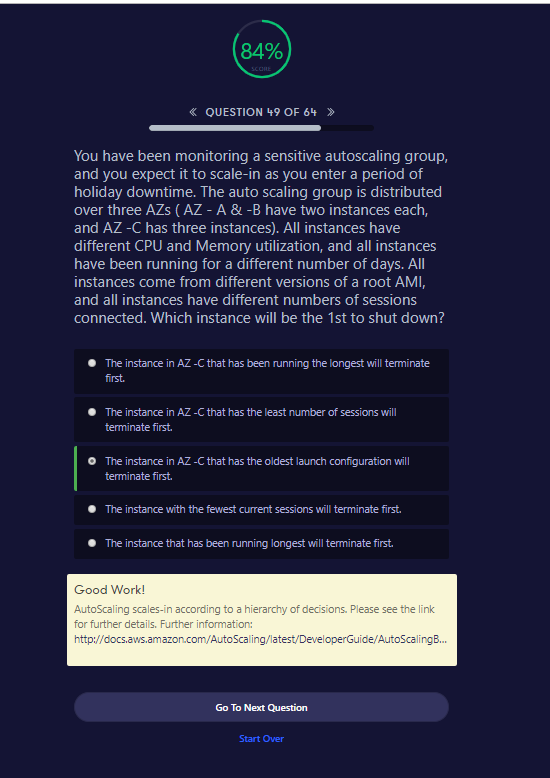
Go To Next QuestionStart Over



Sorry!

There are two issues here: how to handle stale data to avoid paying for high provisioned throughput for infrequently used data, and how to design a partition key that will distribute IO from sequential data across partitions evenly to avoid performance bottlenecks. Further information: <http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GuidelinesForTables.html#GuidelinesForTables.Partitions><http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.Partitions.html><https://aws.amazon.com/blogs/aws/optimizing-provisioned-throughput-in-amazon-dynamodb/>

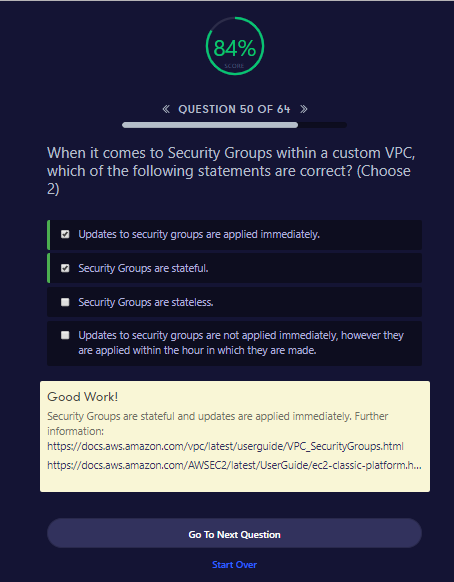
Go To Next QuestionStart Over



Good Work!

AutoScaling scales-in according to a hierarchy of decisions. Please see the link for further details. Further information: <http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AutoScalingBehavior.InstanceTermination.html>

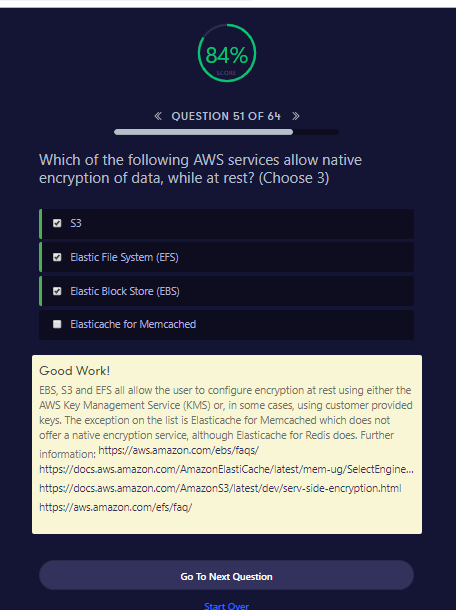
Go To Next QuestionStart Over



Good Work!

Security Groups are stateful and updates are applied immediately. Further information: <https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html><https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-classic-platform.html>

Go To Next QuestionStart Over



##### Good Work!

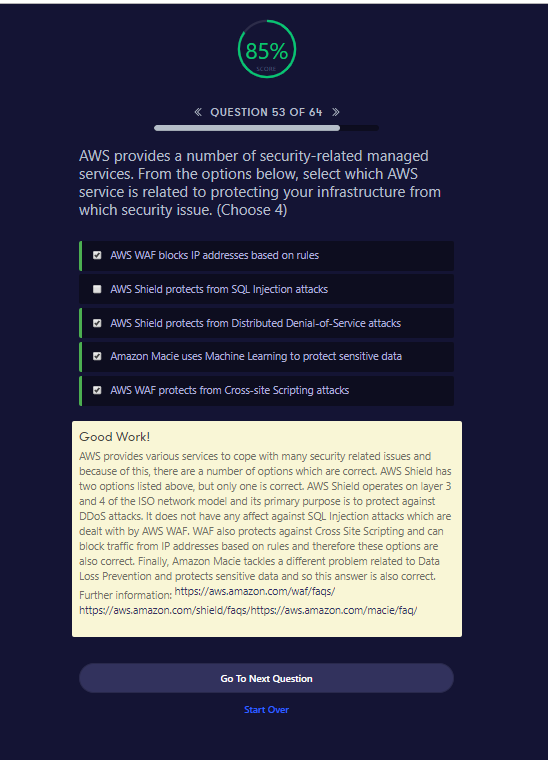
EBS, S3 and EFS all allow the user to configure encryption at rest using either the AWS Key Management Service (KMS) or, in some cases, using customer provided keys. The exception on the list is Elasticache for Memcached which does not offer a native encryption service, although Elasticache for Redis does. Further information: <https://aws.amazon.com/ebs/faqs/><https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/SelectEngine.html><https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html><https://aws.amazon.com/efs/faq/>



Good Work!

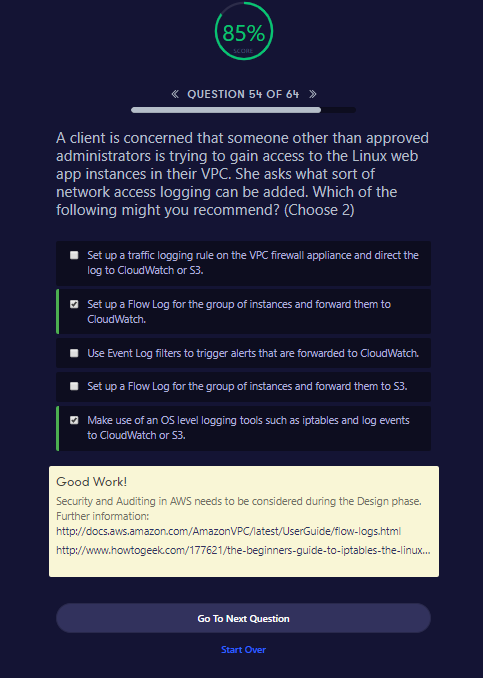
Network throughput is the obvious bottleneck. You are not told in this question whether the proxy server is in a public or private subnet. If it is in a public subnet, the proxy server instance size itself may not be large enough to cope with the current network throughput. If the proxy server is in a private subnet, then it must be using a NAT instance or NAT gateway to communicate out to the internet. If it is a NAT instance, this may also be inadequately provisioned in terms of size. You should therefore increase the size of the proxy server and/or the NAT solution. Further information: <https://aws.amazon.com/articles/2781451301784570><https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-comparison.html>

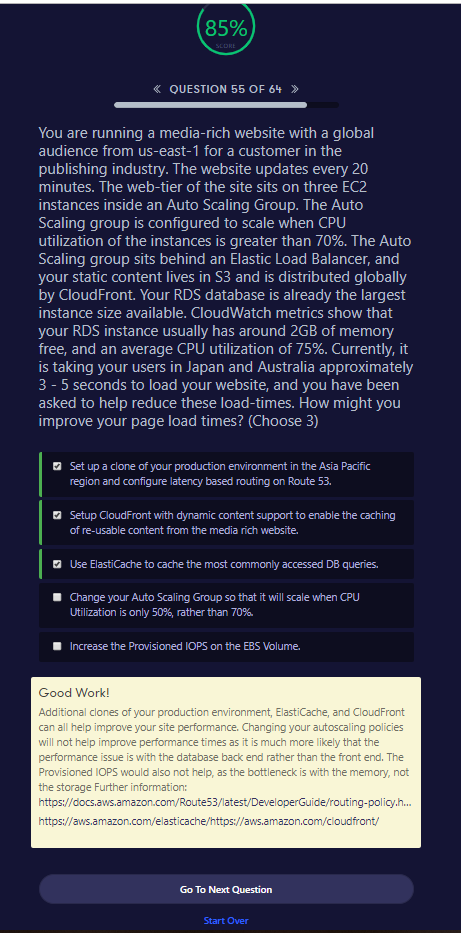
Go To Next QuestionStart Over



##### Good Work!

AWS provides various services to cope with many security related issues and because of this, there are a number of options which are correct. AWS Shield has two options listed above, but only one is correct. AWS Shield operates on layer 3 and 4 of the ISO network model and its primary purpose is to protect against DDoS attacks. It does not have any affect against SQL Injection attacks which are dealt with by AWS WAF. WAF also protects against Cross Site Scripting and can block traffic from IP addresses based on rules and therefore these options are also correct. Finally, Amazon Macie tackles a different problem related to Data Loss Prevention and protects sensitive data and so this answer is also correct. Further information: <https://aws.amazon.com/waf/faqs/><https://aws.amazon.com/shield/faqs/><https://aws.amazon.com/macie/faq/>

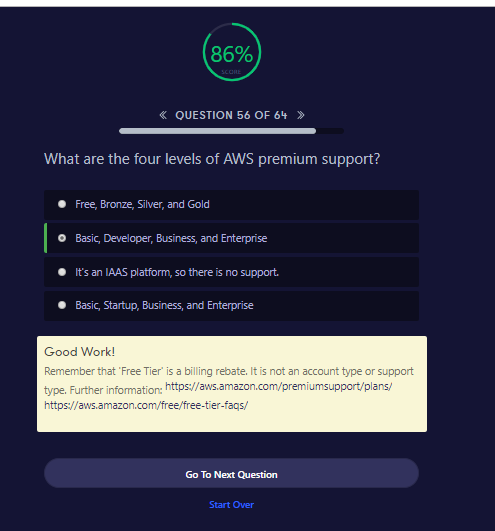




Good Work!

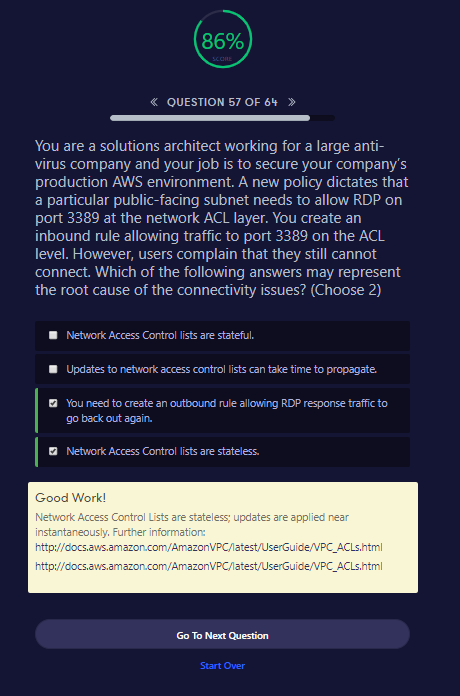
Additional clones of your production environment, ElastiCache, and CloudFront can all help improve your site performance. Changing your autoscaling policies will not help improve performance times as it is much more likely that the performance issue is with the database back end rather than the front end. The Provisioned IOPS would also not help, as the bottleneck is with the memory, not the storage Further information: <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-failover><https://aws.amazon.com/elasticache/><https://aws.amazon.com/cloudfront/>

Go To Next QuestionStart Over



##### Good Work!

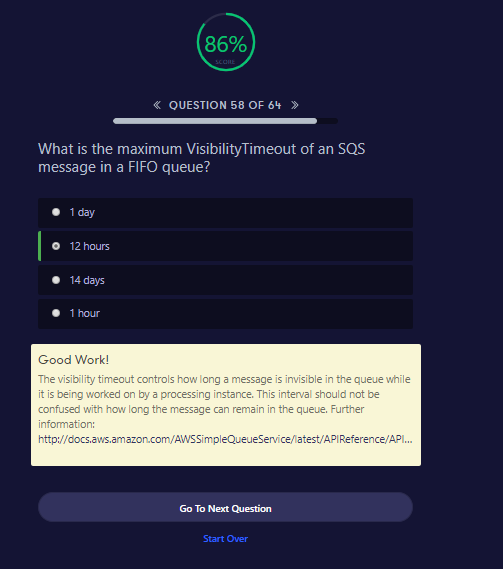
Remember that 'Free Tier' is a billing rebate. It is not an account type or support type. Further information: <https://aws.amazon.com/premiumsupport/plans/><https://aws.amazon.com/free/free-tier-faqs/>

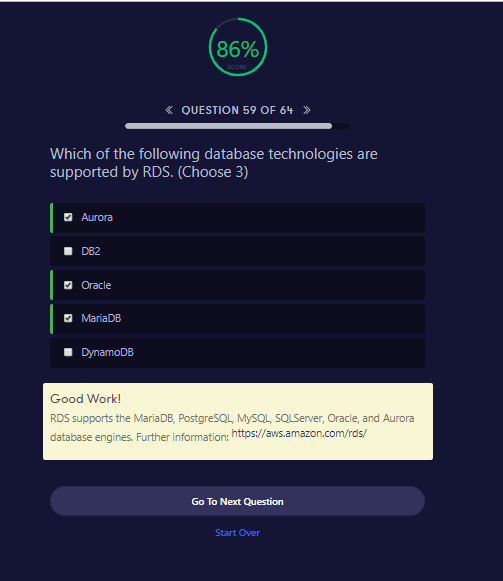


Good Work!

Network Access Control Lists are stateless; updates are applied near instantaneously. Further information: [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\_ACLs.htmlhttp://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\_ACLs.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)

Go To Next QuestionStart Over

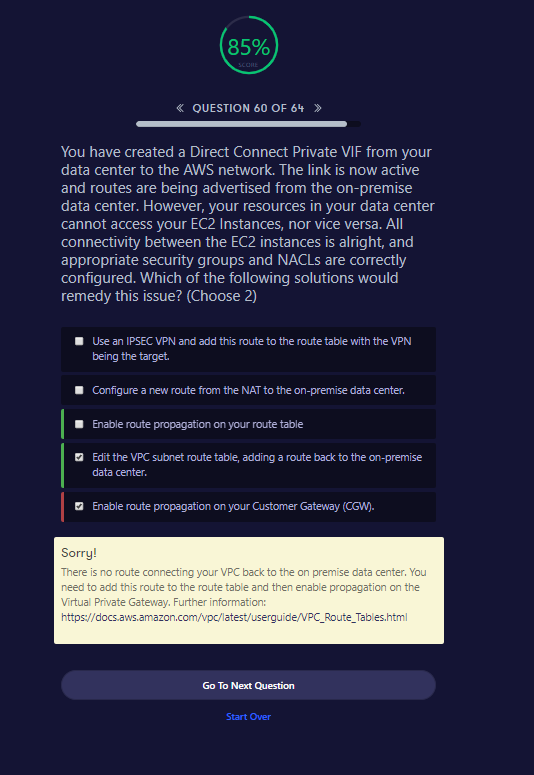




Good Work!

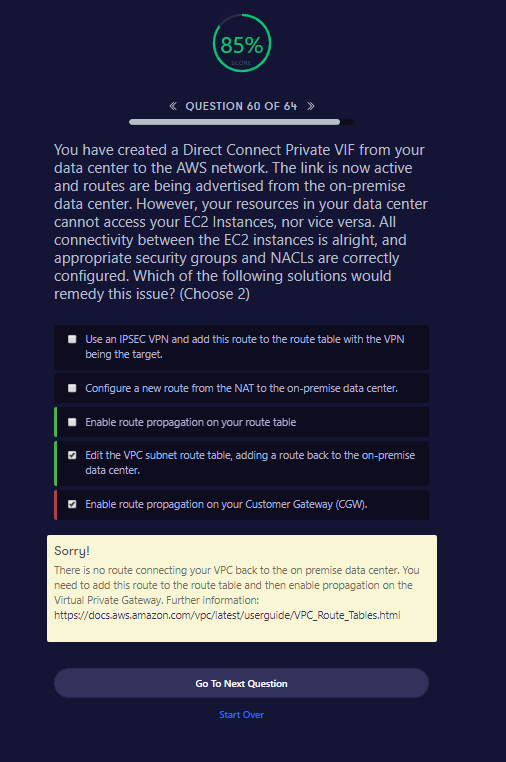
RDS supports the MariaDB, PostgreSQL, MySQL, SQLServer, Oracle, and Aurora database engines. Further information: <https://aws.amazon.com/rds/>

Go To Next QuestionStart Over



##### Sorry!

There is no route connecting your VPC back to the on premise data center. You need to add this route to the route table and then enable propagation on the Virtual Private Gateway. Further information: <https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html>

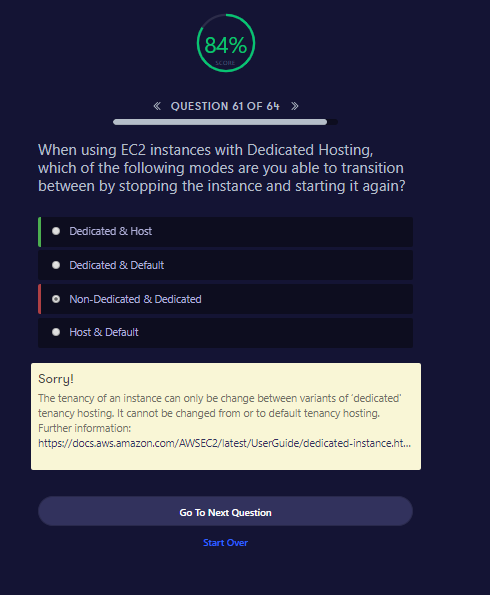


Sorry!

There is no route connecting your VPC back to the on premise data center. You need to add this route to the route table and then enable propagation on the Virtual Private Gateway. Further information: <https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html>

Go To Next QuestionStart Over

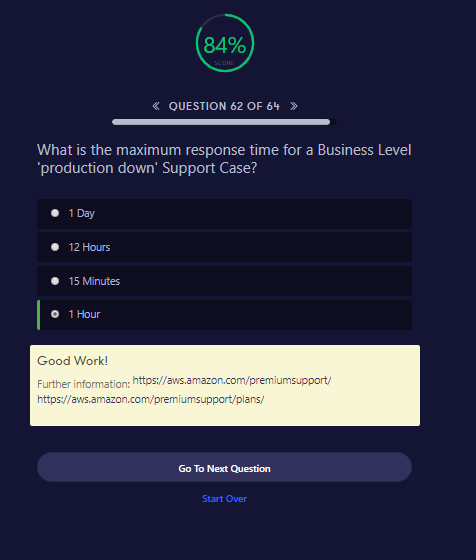
|  |
| --- |
| What is AWS Site-to-Site VPN? https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\_VPN.html https://docs.aws.amazon.com/vpc/latest/userguide/vpn-connections.html https://docs.aws.amazon.com/vpc/latest/adminguide/Introduction.html |
| **Route Propogation https://docs.aws.amazon.com/vpc/latest/userguide/VPC\_Route\_Tables.html** |

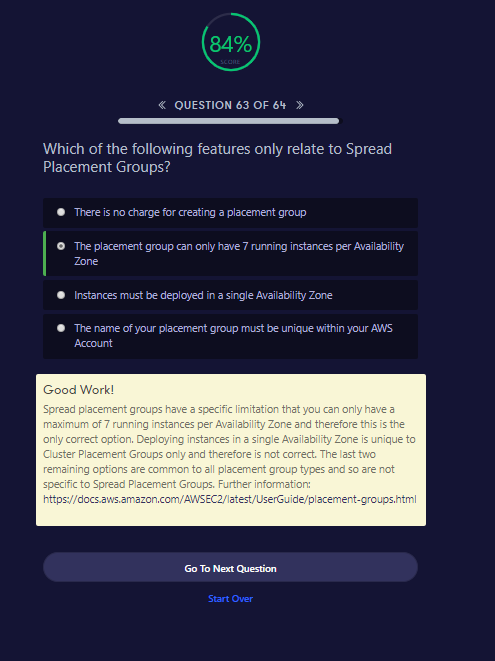


Sorry!

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: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html>

Go To Next QuestionStart Over





Good Work!

Spread placement groups have a specific limitation that you can only have a maximum of 7 running instances per Availability Zone and therefore this is the only correct option. Deploying instances in a single Availability Zone is unique to Cluster Placement Groups only and therefore is not correct. The last two remaining options are common to all placement group types and so are not specific to Spread Placement Groups. Further information: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Go To Next QuestionStart Over

