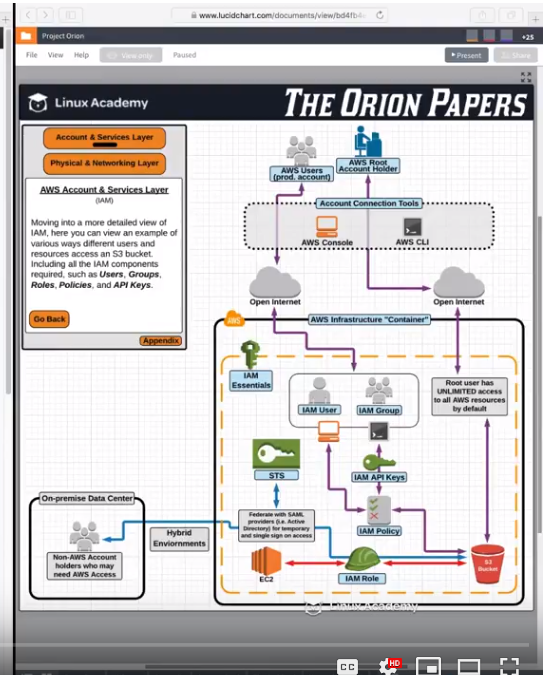


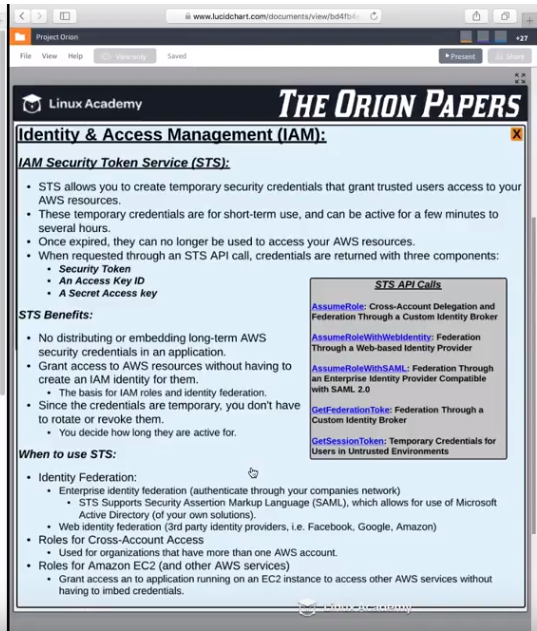
<https://www.youtube.com/watch?v=9e2DdGT5mZg> – Good

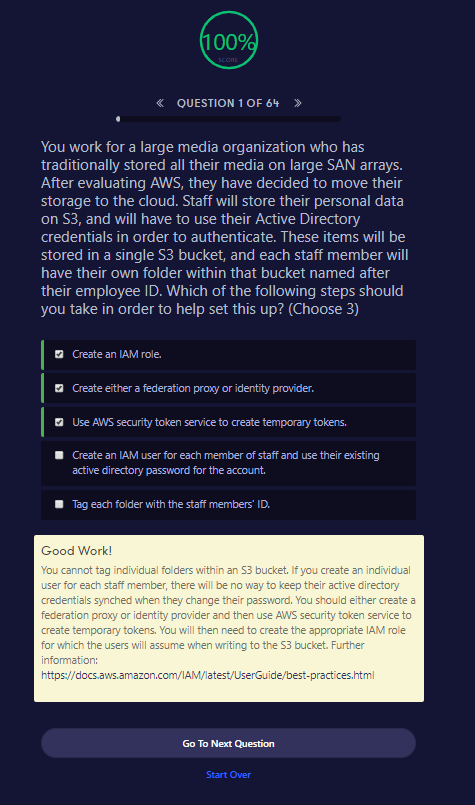
<https://www.youtube.com/watch?v=4_csSXc_GNU> – OKAY

<https://medium.com/@devopslearning/introduction-to-aws-security-token-service-sts-b3049aade3c1>

<https://www.youtube.com/watch?v=4cxSqMHgDGs> – GREAT ONE







Good Work!

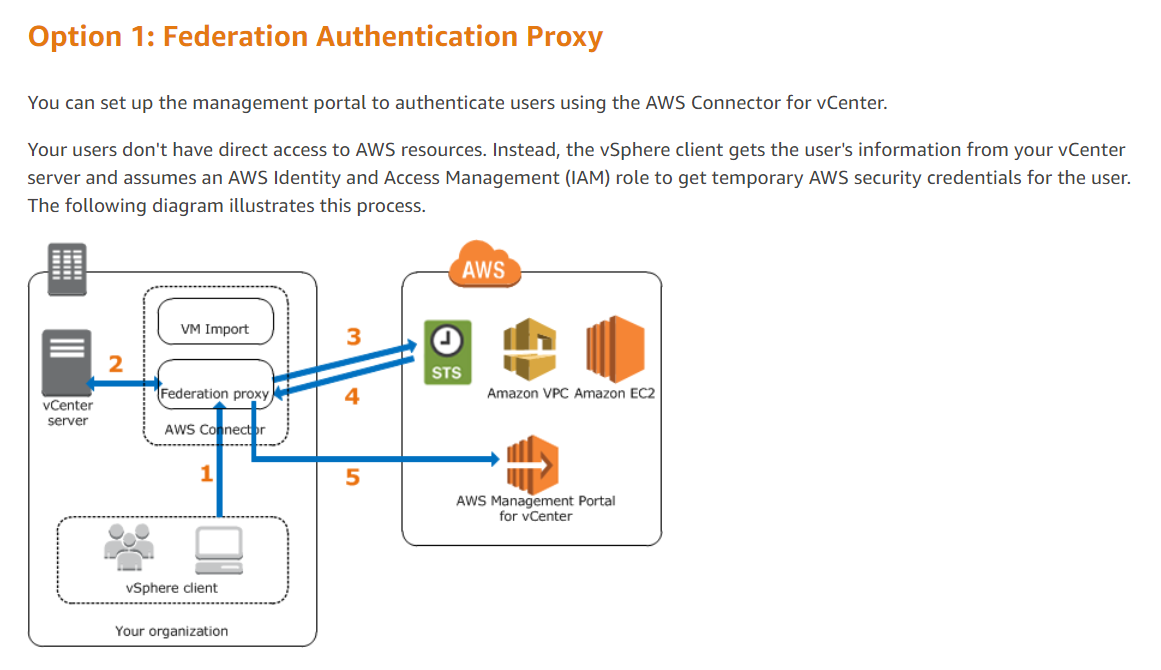
You cannot tag individual folders within an S3 bucket. If you create an individual user for each staff member, there will be no way to keep their active directory credentials synched when they change their password. You should either create a federation proxy or identity provider and then use AWS security 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>

<https://docs.aws.amazon.com/amp/latest/userguide/install-option-connector.html>

# Option 1: Federation Authentication Proxy

You can set up the management portal to authenticate users using the AWS Connector for vCenter.

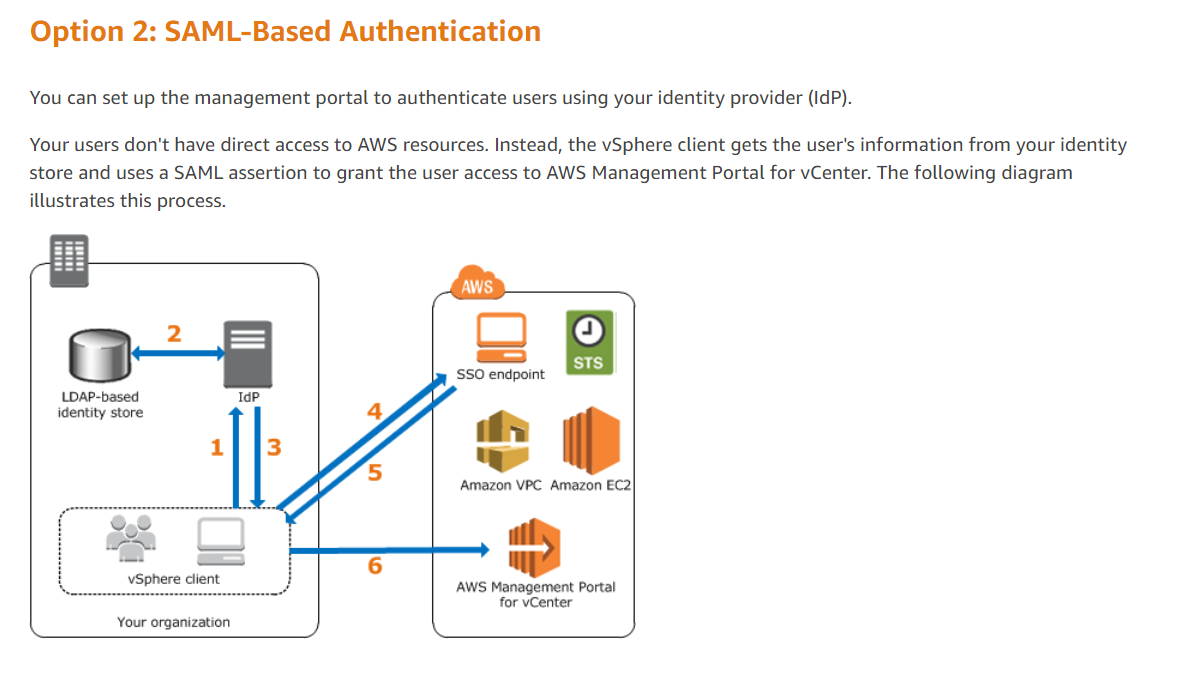
Your users don't have direct access to AWS resources. Instead, the vSphere client gets the user's information from your vCenter server and assumes an AWS Identity and Access Management (IAM) role to get temporary AWS security credentials for the user. The following diagram illustrates this process.



# Option 2: SAML-Based Authentication

You can set up the management portal to authenticate users using your identity provider (IdP).

Your users don't have direct access to AWS resources. Instead, the vSphere client gets the user's information from your identity store and uses a SAML assertion to grant the user access to AWS Management Portal for vCenter. The following diagram illustrates this process.

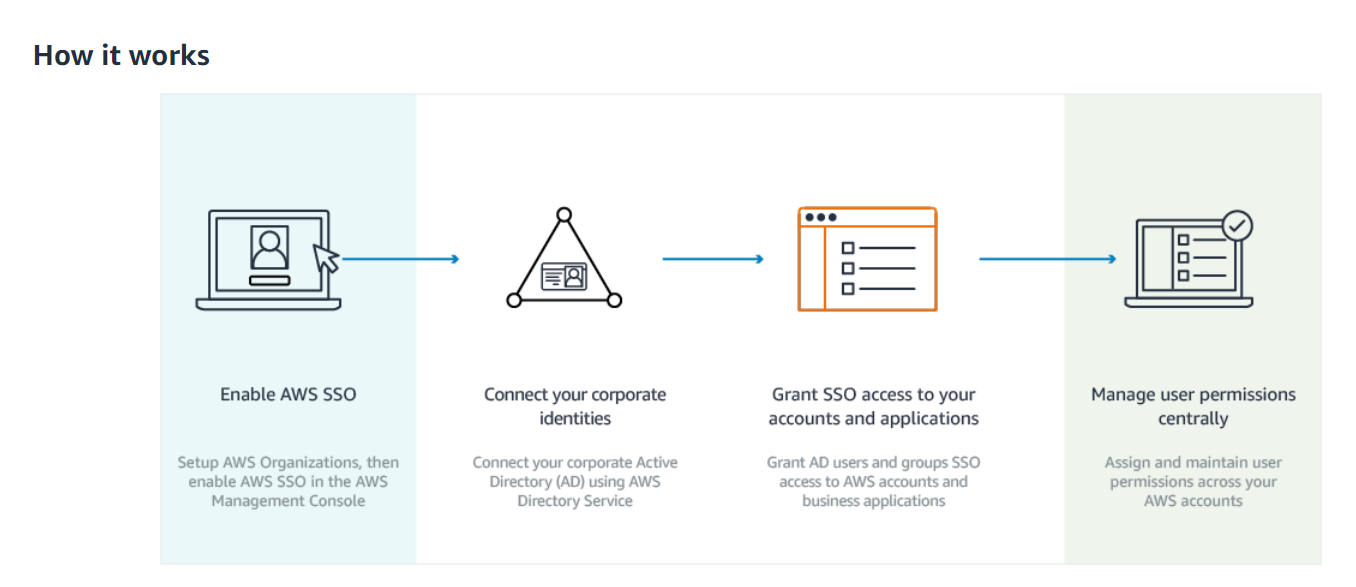


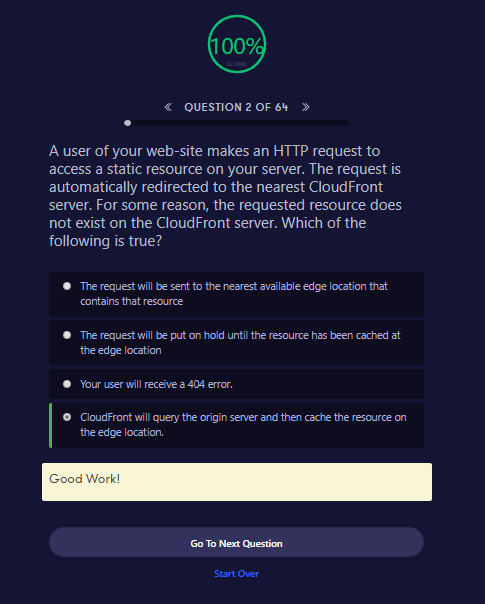
What is AWS SSO?

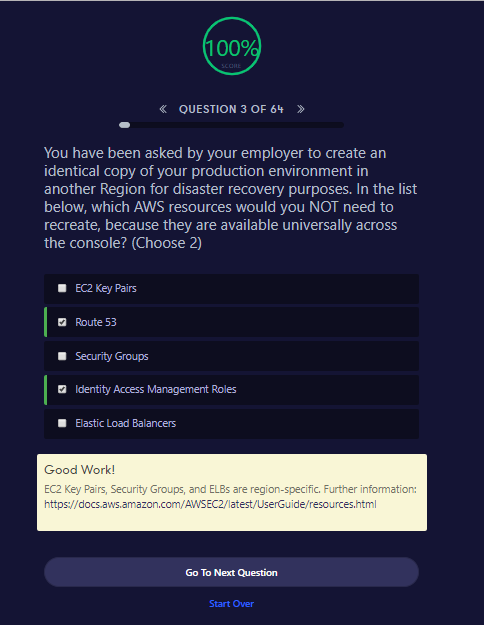
**AWS Single Sign-On** (**AWS SSO**) is a cloud service that allows you to grant your users access to **AWS** resources, such as Amazon EC2 instances, across multiple **AWS** accounts. ... You can now create your users centrally in **AWS SSO** and manage user access to all your **AWS** accounts and applications.Oct 17, 2018

How does AWS SSO work?

Centrally manage single sign-on (**SSO**) access to multiple **AWS** accounts and business applications. ... With just a few clicks, you **can** enable a highly available **SSO** service without the upfront investment and on-going maintenance costs of operating your own **SSO** infrastructure.Oct 30, 2018

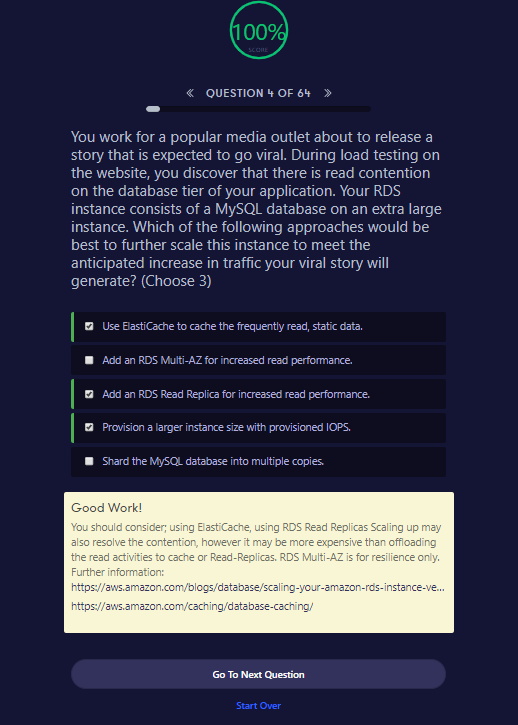






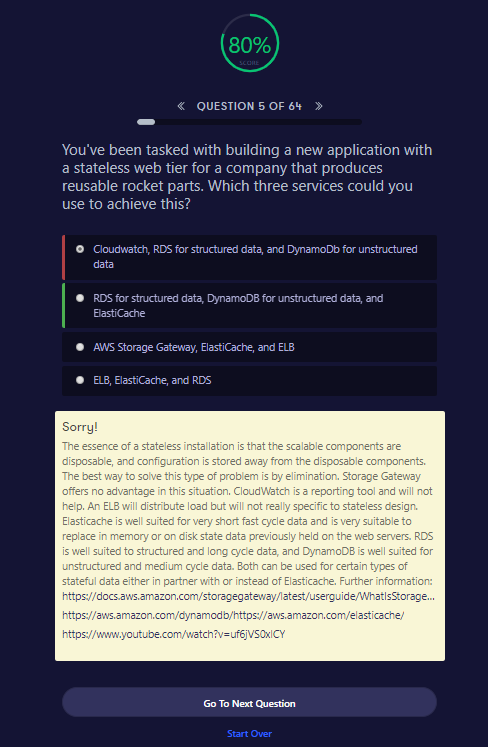
##### Good Work!

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



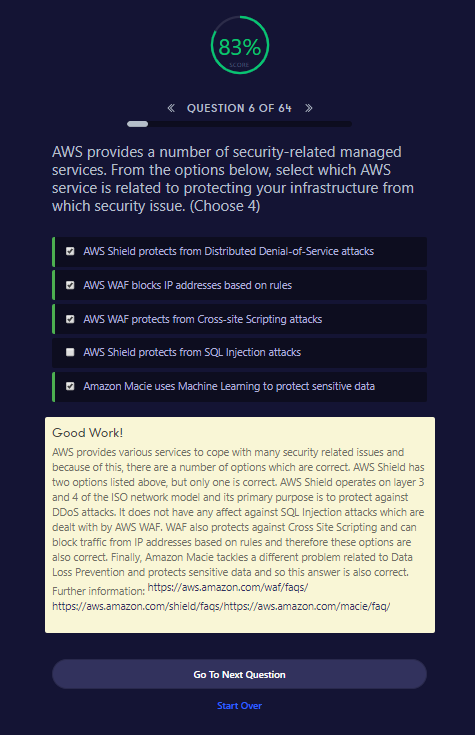
##### Good Work!

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/>



##### Sorry!

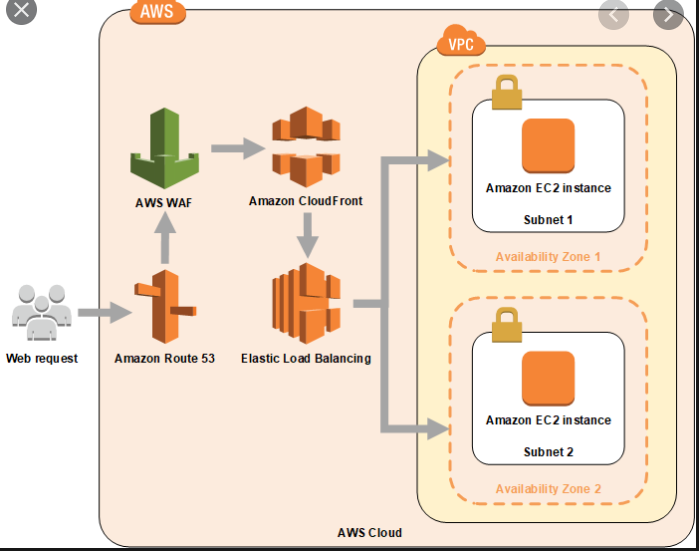
The essence of a stateless installation is that the scalable components are disposable, and configuration is stored away from the disposable components. The best way to solve this type of problem is by elimination. Storage Gateway offers no advantage in this situation. CloudWatch is a reporting tool 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>

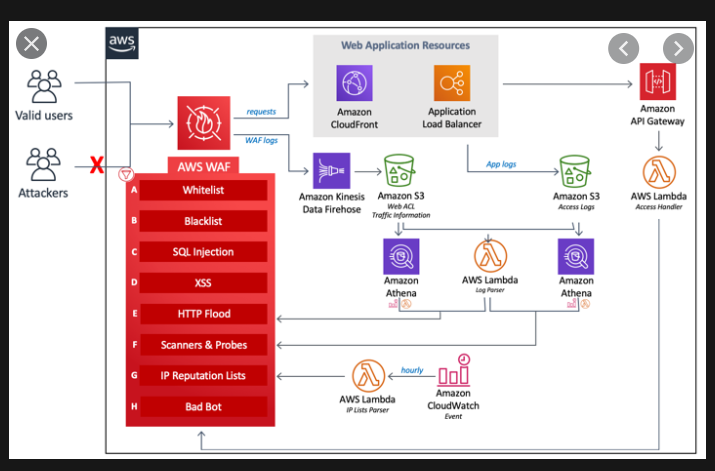


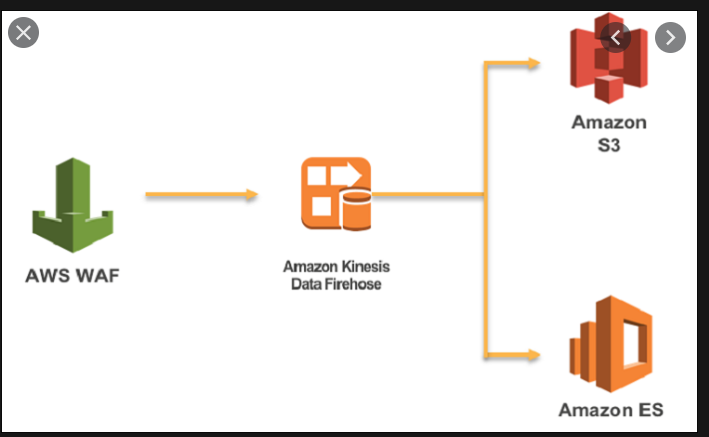
##### Good Work!

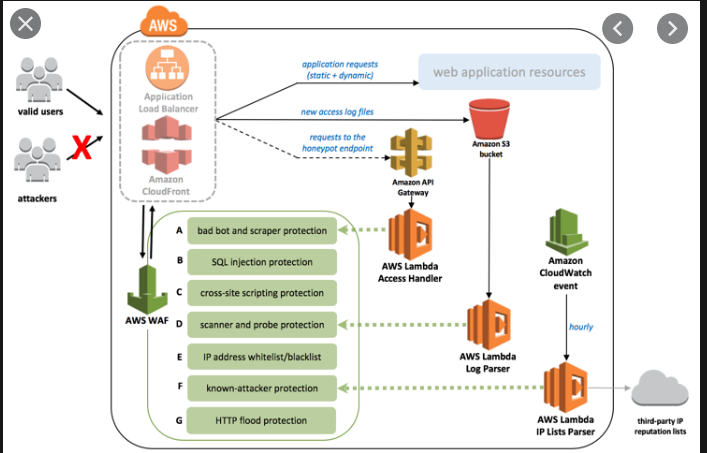
AWS provides various services to cope with many security related issues and because of this, there are a number of options which are correct. AWS Shield has two options listed above, but only one is correct. AWS Shield operates on layer 3 and 4 of the ISO network model and its primary purpose is to protect 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/>

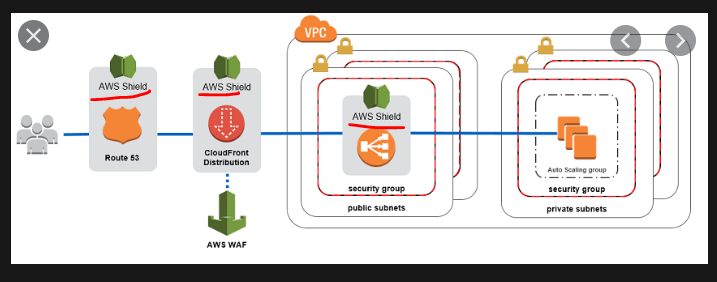
AWS WAF

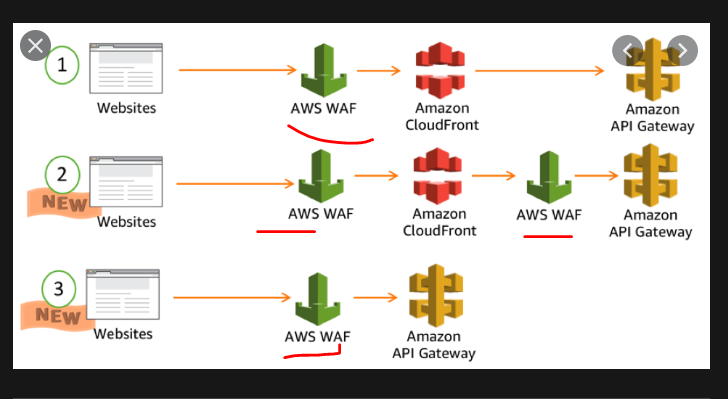


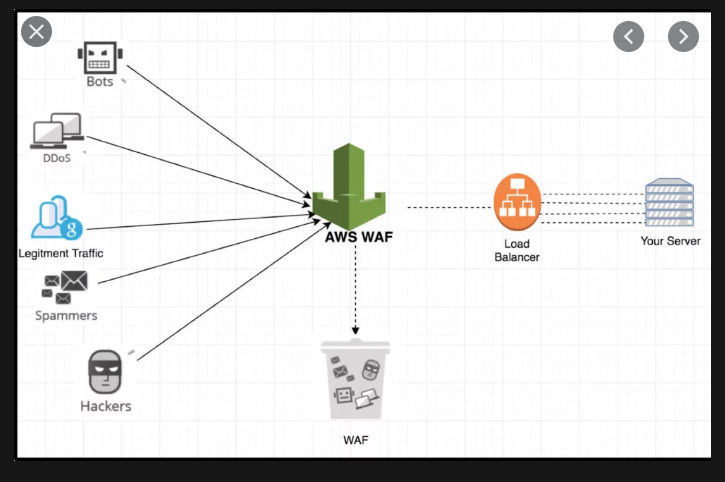








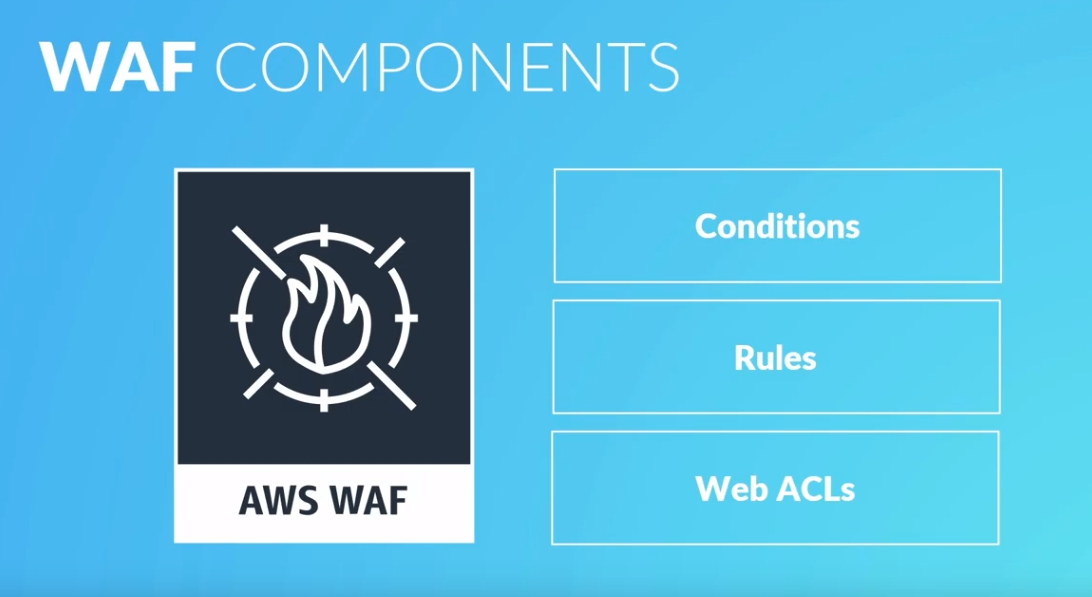


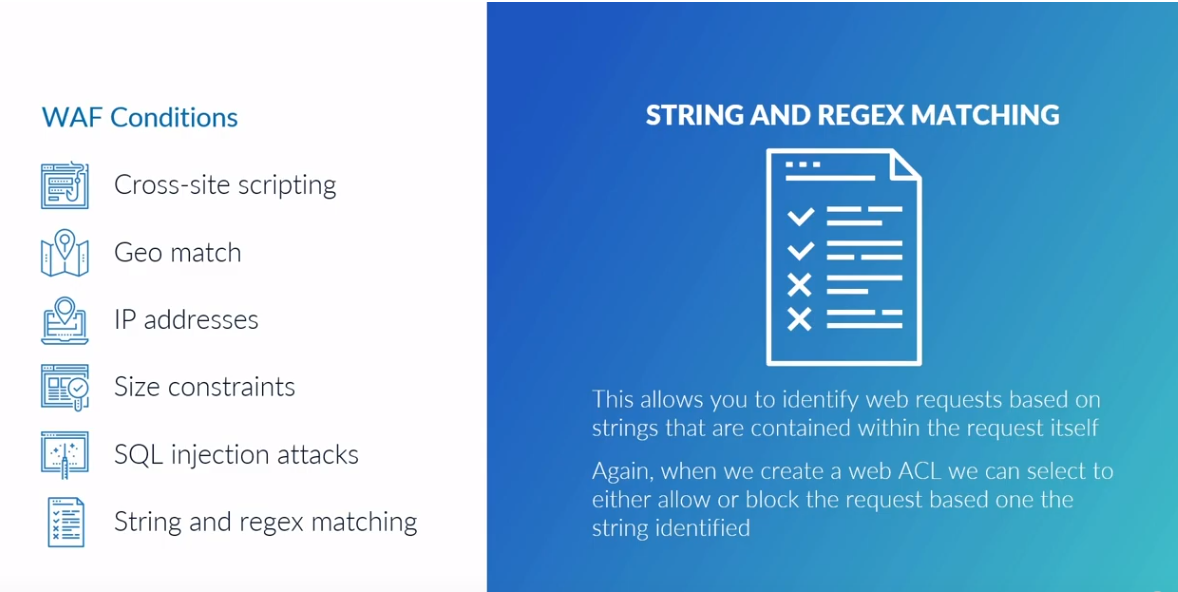


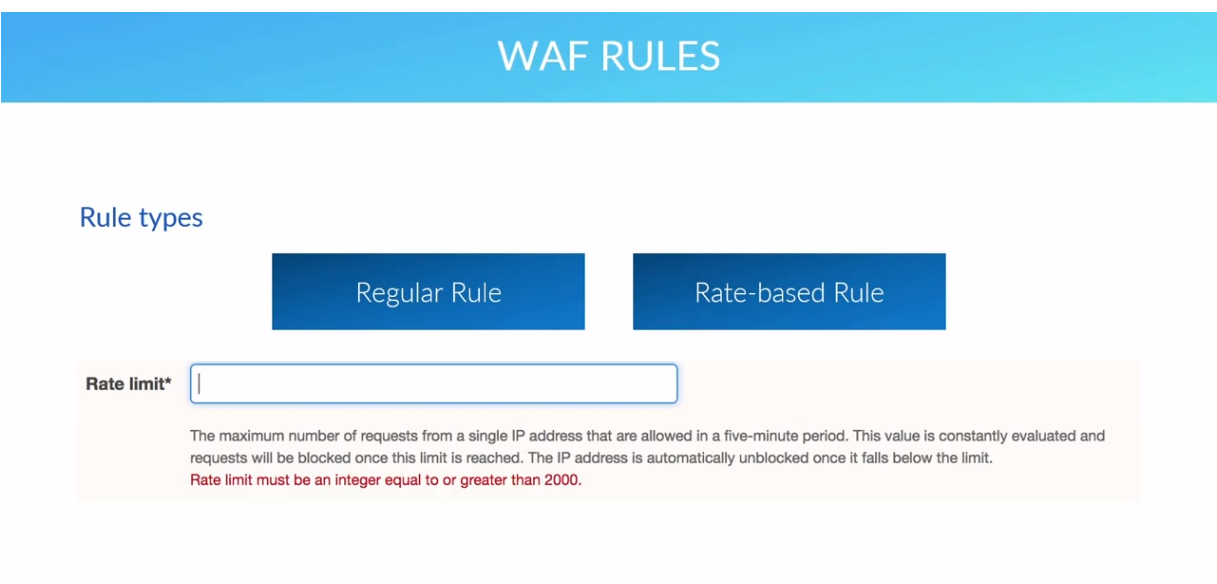


- Protects from SQL Injection

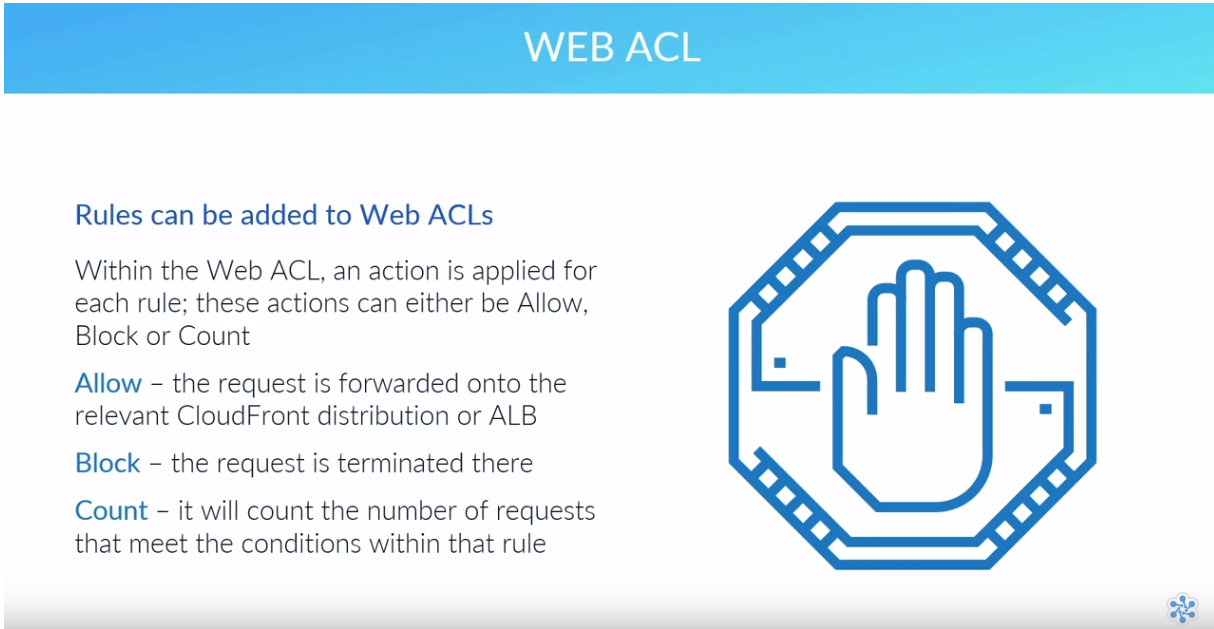
- Protects from Cross site scripting

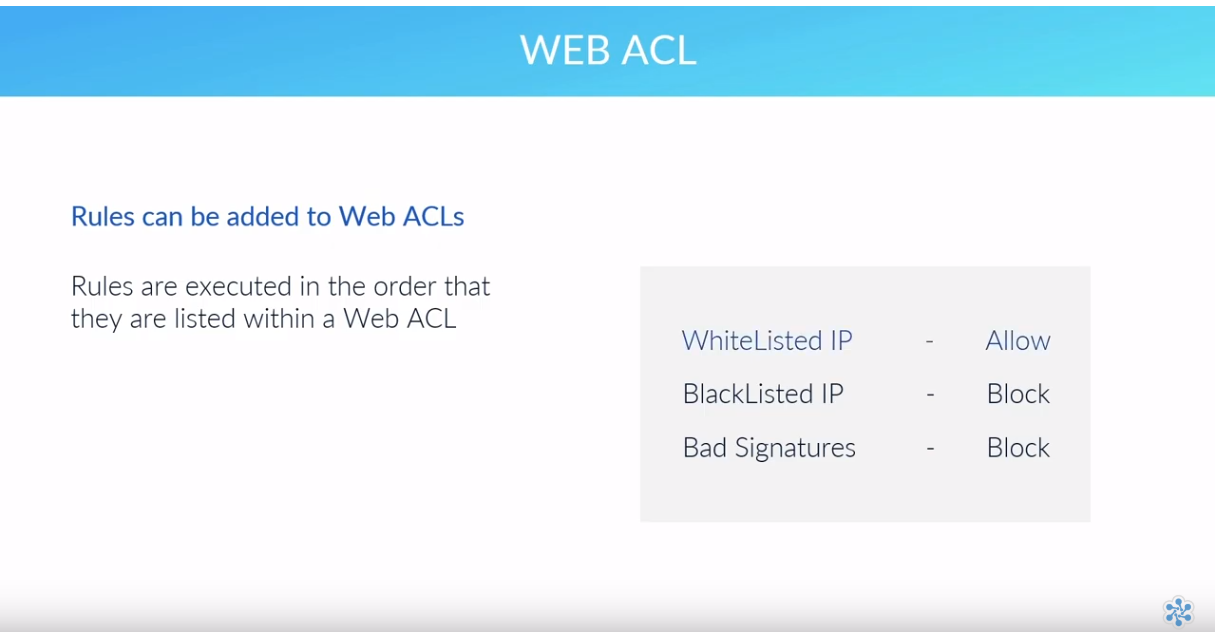


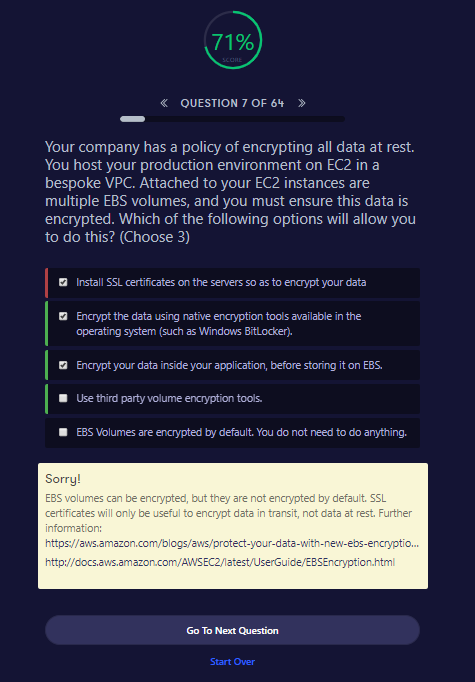






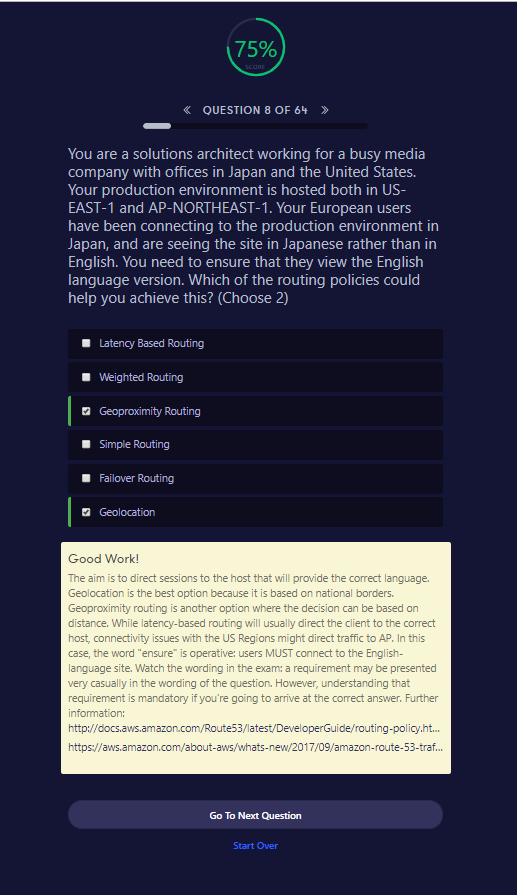






##### Sorry!

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 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/>

Latency based routing will not ensure same location all the time if there are connectivity issues

Difference between Geolocation and GeoProximity

Geolocation routes user to resources based on the location of the DNS queries and the records setup. So depending on the location of the user you can route (or restrict) them to a specific resource.

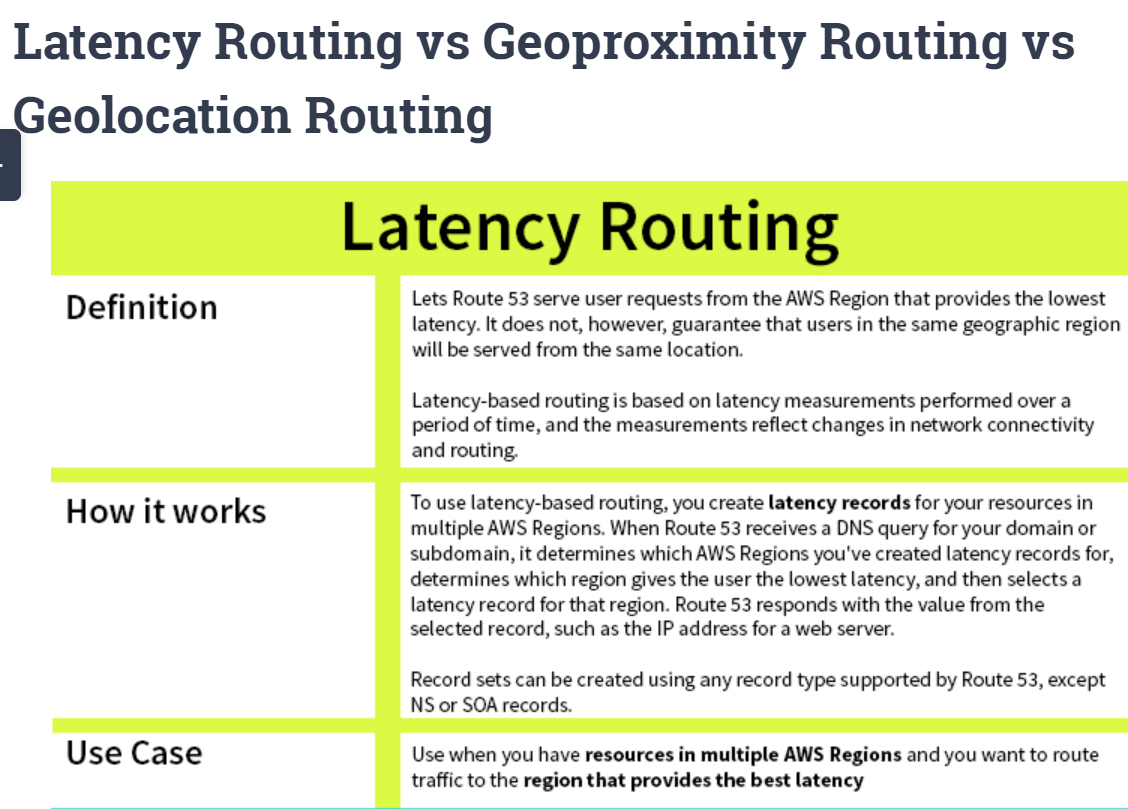
As an example, you have web servers in London, England and other in Frankfurt, Germany. There is a user in Lille, France which is closer to London. You can create a record which directs users in mainland Europe get to the Frankfurt webservers. So our user in Lille will be directed to the in Frankfurt.

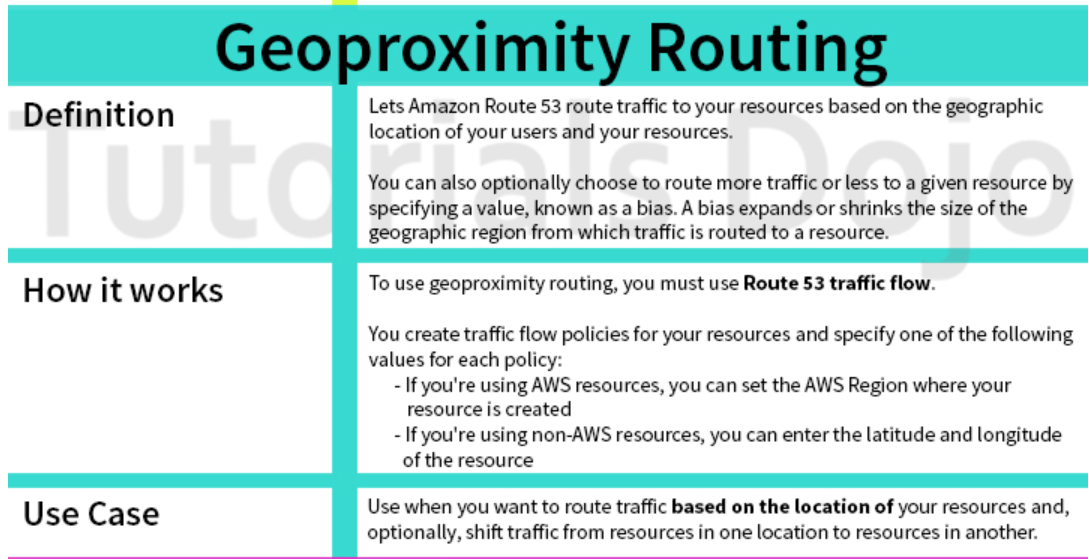
Geoproximity can be thought of allocating a sphere of influence to resources based on the bias you give the resource, determining which resources users get directed to.

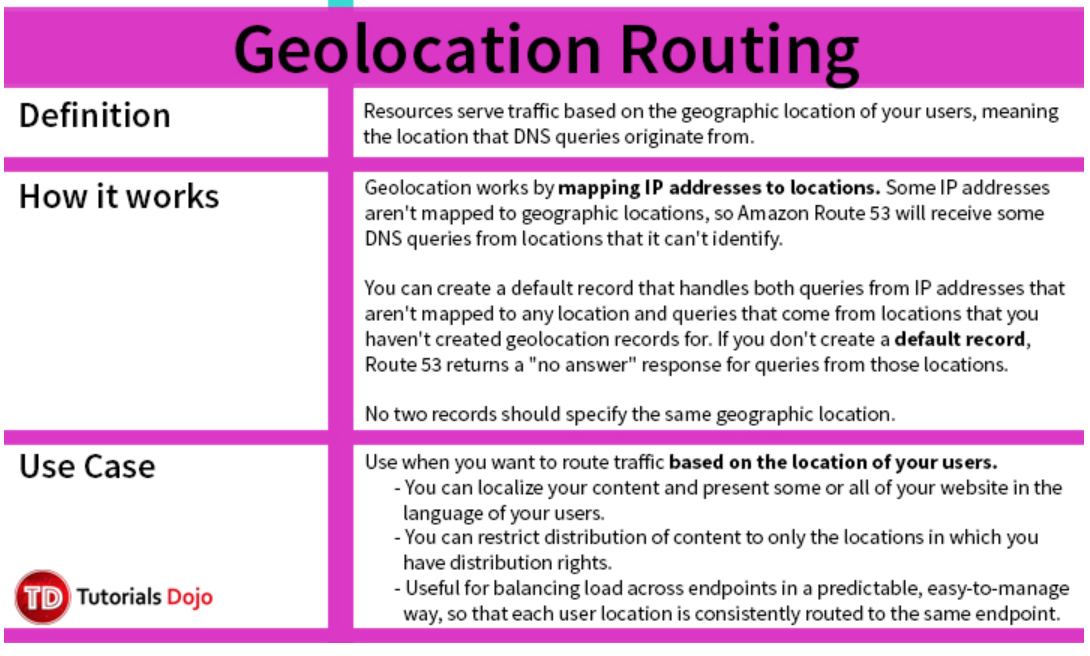
Using the example, you can allocate a greater basis to Frankfurt which means the user in Lille will be routed to that resource over London. Achieving the same result but using differ mechanism.

A better use case (in my opinion) for Geoproximity is if you have more resources/bigger instance size in a particular region, hence why you would want to direct users to that region over other.

<https://tutorialsdojo.com/latency-routing-vs-geoproximity-routing-vs-geolocation-routing/>







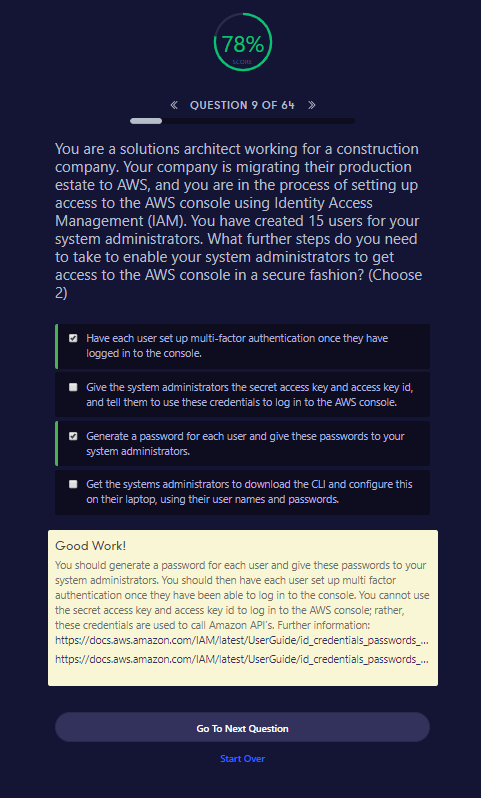
<https://www.whizlabs.com/blog/route-53-policies/>

<http://jayendrapatil.com/aws-route-53-routing-policy/>

## **AWS Certification Exam Practice Questions**

* Questions are collected from Internet and the answers are marked as per my knowledge and understanding (which might differ with yours).
* AWS services are updated everyday and both the answers and questions might be outdated soon, so research accordingly.
* AWS exam questions are not updated to keep up the pace with AWS updates, so even if the underlying feature has changed the question might not be updated
* Open to further feedback, discussion and correction.

1. You have deployed a web application targeting a global audience across multiple AWS Regions under the domain name example.com. You decide to use Route 53 Latency-Based Routing to serve web requests to users from the region closest to the user. To provide business continuity in the event of server downtime you configure weighted record sets associated with two web servers in separate Availability Zones per region. During a DR test you notice that when you disable all web servers in one of the regions Route 53 does not automatically direct all users to the other region. What could be happening? (Choose 2 answers)
   1. Latency resource record sets cannot be used in combination with weighted resource record sets.
   2. **You did not setup an http health check for one or more of the weighted resource record sets associated with the disabled web servers**
   3. The value of the weight associated with the latency alias resource record set in the region with the disabled servers is higher than the weight for the other region.
   4. One of the two working web servers in the other region did not pass its HTTP health check
   5. **You did not set “Evaluate Target Health” to “Yes” on the latency alias resource record set associated with example.com in the region where you disabled the servers.**
2. The compliance department within your multi-national organization requires that all data for your customers that reside in the European Union (EU) must not leave the EU and also data for customers that reside in the US must not leave the US without explicit authorization. What must you do to comply with this requirement for a web based profile management application running on EC2?
   1. Run EC2 instances in multiple AWS Availability Zones in single Region and leverage an Elastic Load Balancer with session stickiness to route traffic to the appropriate zone to create their profile (should be in 2 different regions – US and Europe)
   2. Run EC2 instances in multiple Regions and leverage Route 53’s Latency Based Routing capabilities to route traffic to the appropriate region to create their profile (Latency based routing policy would not guarantee the compliance requirement)
   3. **Run EC2 instances in multiple Regions and leverage a third party data provider to determine if a user needs to be redirect to the appropriate region to create their profile**
   4. Run EC2 instances in multiple AWS Availability Zones in a single Region and leverage a third party data provider to determine if a user needs to be redirect to the appropriate zone to create their profile(should be in 2 different regions – US and Europe)
3. A US-based company is expanding their web presence into Europe. The company wants to extend their AWS infrastructure from Northern Virginia (us-east-1) into the Dublin (eu-west-1) region. Which of the following options would enable an equivalent experience for users on both continents?
   1. Use a public-facing load balancer per region to load-balance web traffic, and enable HTTP health checks.
   2. Use a public-facing load balancer per region to load-balance web traffic, and enable sticky sessions.
   3. **Use Amazon Route 53, and apply a geolocation routing policy to distribute traffic across both regions**
   4. Use Amazon Route 53, and apply a weighted routing policy to distribute traffic across both regions.
4. You have been asked to propose a multi-region deployment of a web-facing application where a controlled portion of your traffic is being processed by an alternate region. Which configuration would achieve that goal?
   1. **Route 53 record sets with weighted routing policy**
   2. Route 53 record sets with latency based routing policy
   3. Auto Scaling with scheduled scaling actions set
   4. Elastic Load Balancing with health checks enabled
5. Your company is moving towards tracking web page users with a small tracking image loaded on each page. Currently you are serving this image out of us-east, but are starting to get concerned about the time it takes to load the image for users on the west coast. What are the two best ways to speed up serving this image? Choose 2 answers
   1. **Use Route 53’s Latency Based Routing and serve the image out of us-west-2 as well as us-east-1**
   2. **Serve the image out through CloudFront**
   3. Serve the image out of S3 so that it isn’t being served of your web application tier
   4. Use EBS PIOPs to serve the image faster out of your EC2 instances
6. Your API requires the ability to stay online during AWS regional failures. Your API does not store any state, it only aggregates data from other sources – you do not have a database. What is a simple but effective way to achieve this uptime goal?
   1. Use a CloudFront distribution to serve up your API. Even if the region your API is in goes down, the edge locations CloudFront uses will be fine.
   2. Use an ELB and a cross-zone ELB deployment to create redundancy across datacenters. Even if a region fails, the other AZ will stay online.
   3. Create a Route53 Weighted Round Robin record, and if one region goes down, have that region redirect to the other region.
   4. **Create a Route53 Latency Based Routing Record with Failover and point it to two identical deployments of your stateless API in two different regions. Make sure both regions use Auto Scaling Groups behind ELBs.** (Refer [link](http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html))



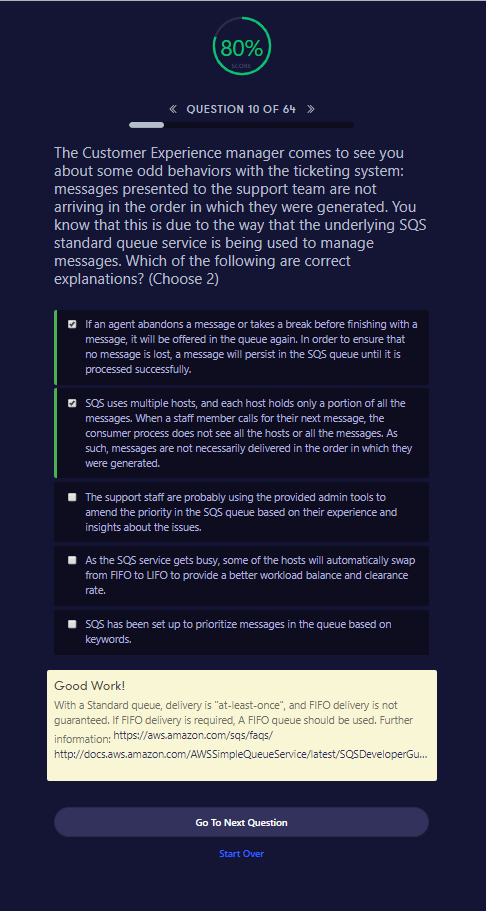
##### Good Work!

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>

Clearly explained here

<https://www.sweetprocess.com/procedures/_eG30mkvYDrfAmevj78A0i6E1GZE/add-an-administrator-to-your-amazon-aws-account/>

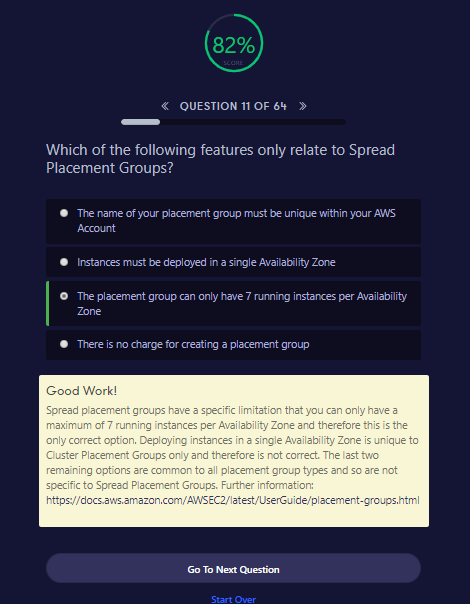
SECURITY PILLAR READ IT



##### 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>

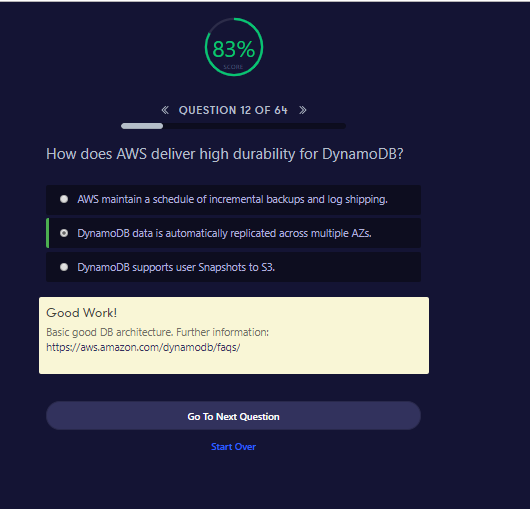
Go To Next QuestionStart Over



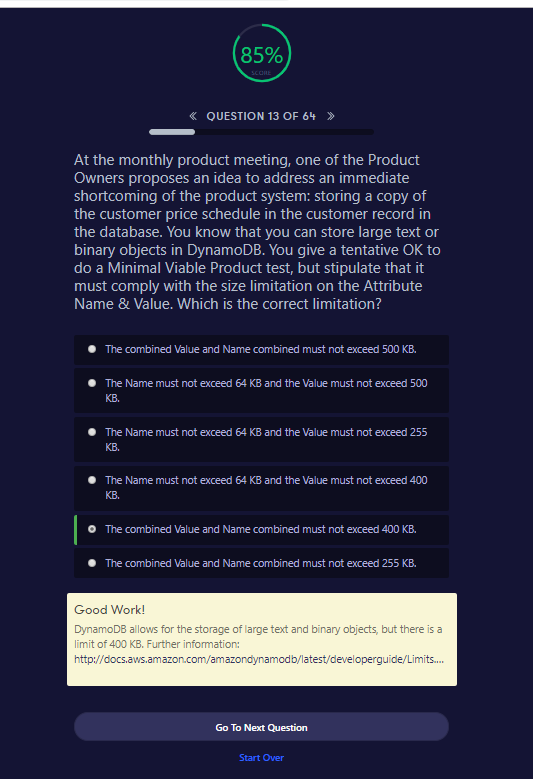
##### Good Work!

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>

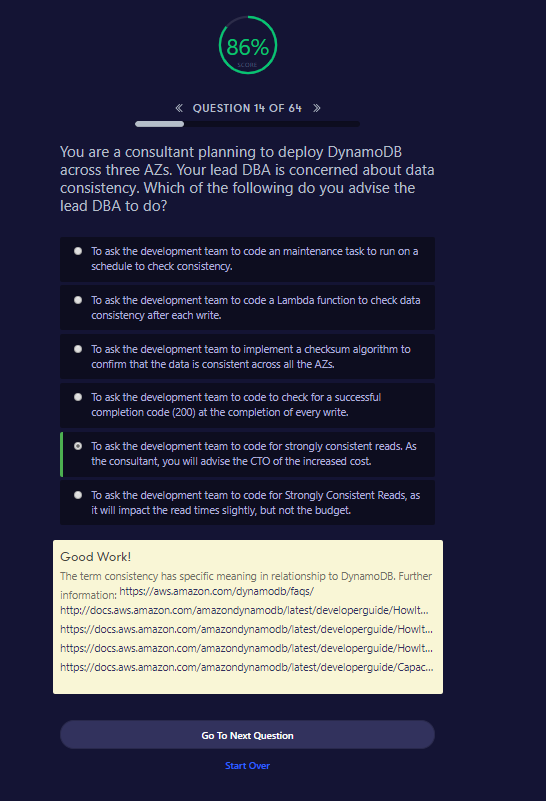
Go To Next QuestionStart Over



All DB comparisions

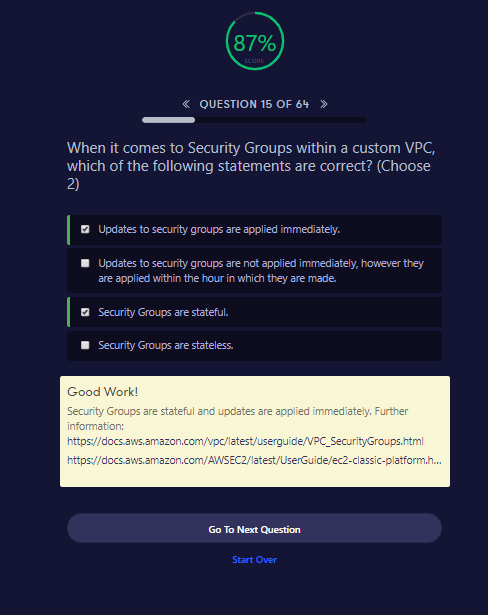


<https://news.ycombinator.com/item?id=8428791>



##### 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!

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>