**Content**

[1. Reddit tips for the exam 2](#_Toc68695674)

[1. EC2Rescue tool with System status checks 2](#_Toc68695675)

[2. SSM deep dive [todo] 2](#_Toc68695676)

[3. Hybrid networking with backup 2](#_Toc68695677)

[4. When to use what storage transfer method 2](#_Toc68695678)

[5. Lambda connectivity issue in a VPC 2](#_Toc68695679)

[6. IAM advanced 2](#_Toc68695680)

[7. Schema Conversion Tool (SCT) 2](#_Toc68695681)

[8. VPC Peering that uses Longest Prefix Match 3](#_Toc68695682)

[9. Private Hosted Zone 3](#_Toc68695683)

[2. Whizlabs practice test 4 4](#_Toc68695684)

[1. Ec2 instance hibernation 4](#_Toc68695685)

[2. Elastic MapReduce 4](#_Toc68695686)

[3. EC2Launch v2, EC2Launch, EC2Config 8](#_Toc68695687)

[4. The question tricks to fool you 8](#_Toc68695688)

[3. Whizlabs practice test 3 9](#_Toc68695689)

[1. Load Balancers 9](#_Toc68695690)

[3.1.1. Classic 11](#_Toc68695691)

[3.1.2. Application LB 12](#_Toc68695692)

[3.1.3. Network LB 12](#_Toc68695693)

[3.1.4. E2E Encryption 12](#_Toc68695694)

[2. Cloudtrail 13](#_Toc68695695)

1. Reddit tips for the exam
   1. EC2Rescue tool with System status checks

EC2Rescue for EC2 Windows is a troubleshooting tool that you can run on your Amazon EC2 Windows Server instances. Use the tool to troubleshoot OS-level issues and to collect advanced logs and configuration files for further analysis. The following are some common issues that EC2Rescue can address:

* Instance connectivity issues due to firewall, Remote Desktop Protocol (RDP), or network interface configuration.
* OS boot issues due to a blue screen or stop error, a boot loop, or a corrupted registry.
* Any issues that might need advanced log analysis and troubleshooting.
  1. SSM deep dive [todo]
  2. Hybrid networking with backup

Using backup connection line for DirectConnect. Answers will be between VPN or second directConnect, you need to see if question says cheap (VPN) or company requires sensitive latency and highly available.

* 1. When to use what storage transfer method

There was a 500mbps DX bought from partner network and has separate 1gbps internet line always available. Some ~20 TB files needed to transfer and which will be best way? Options had Storage Gateway on DX, S3 upload, S3 transfer acceleration, Snowball... (Tip: In your mind calculate how much each bandwidth can transfer in a day before picking snowball as for some questions transferring large data with Snowball is always not good option).

* 1. Lambda connectivity issue in a VPC

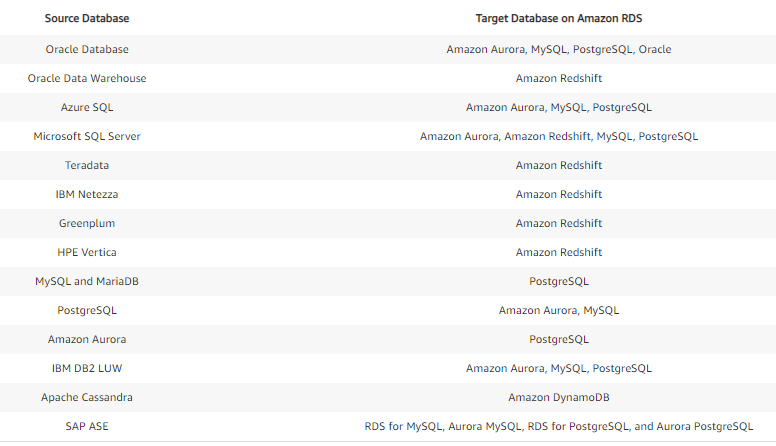
check subnet of lambda has route to NAT gateway

* 1. IAM advanced

Using tags to manage resource like ec2 for multiple business units.( in the same account different unit cant control EC2 of other unit)

* 1. Schema Conversion Tool (SCT)

The AWS Schema Conversion Tool makes heterogeneous database migrations predictable by automatically converting the source database schema and a majority of the database code objects, including views, stored procedures, and functions, to a format compatible with the target database.

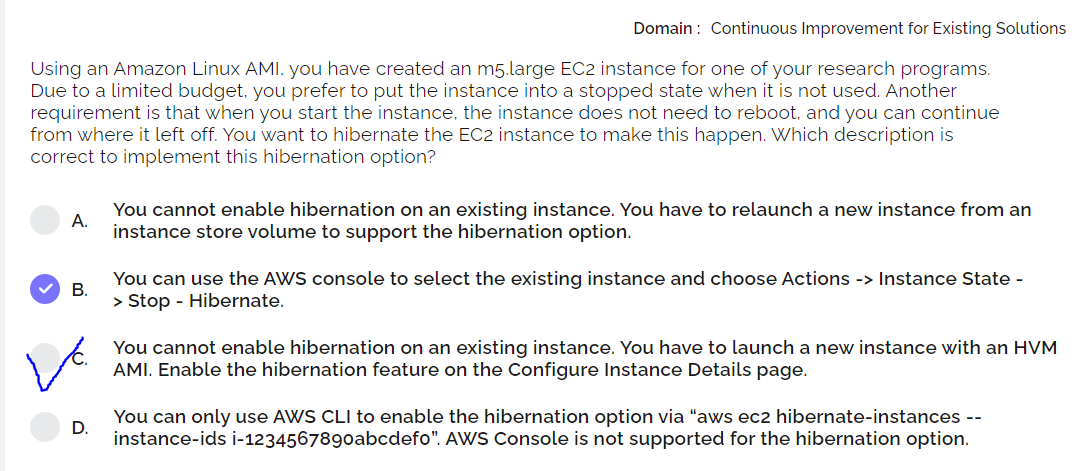


* 1. VPC Peering that uses Longest Prefix Match

<https://aws.amazon.com/blogs/networking-and-content-delivery/influencing-traffic-over-hybrid-networks-using-longest-prefix-match/>

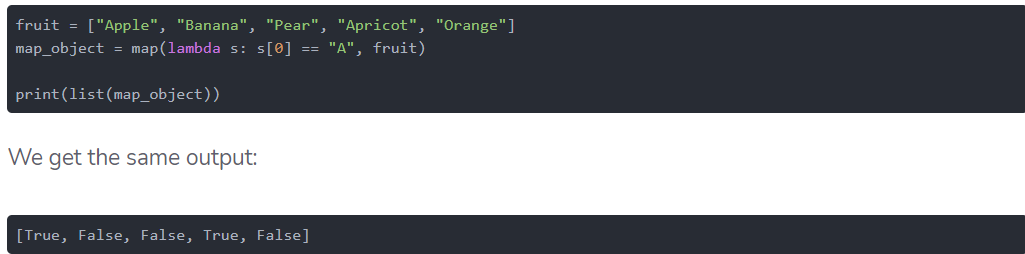
* 1. Private Hosted Zone

1. Whizlabs practice test 4
   1. Ec2 instance hibernation



* Instance store-backed instances cannot be hibernated
* must be an HVM AMI that supports hibernation
* the data on the instance store volumes is lost.
* EBS root volume size - must be large enough to store the RAM contents and accommodate your expected usage, for example, OS or applications.
* EBS root volume encryption - To use hibernation, the root volume must be encrypted to ensure the protection of sensitive content that is in memory at the time of hibernation.
* Enable hibernation at launch - You cannot enable hibernation on an existing instance
* Purchasing options - This feature is available for On-Demand Instances and Reserved Instances. It is not available for Spot Instances.
* You can't change the instance type or size of an instance with hibernation enabled.
* You can't hibernate an instance that is in an Auto Scaling group or used by Amazon ECS.
* recommend disabling KASLR (Kernel Address Space Layout Randomization). On Ubuntu 16.04 LTS or Ubuntu 18.04 LTS
  1. Elastic MapReduce

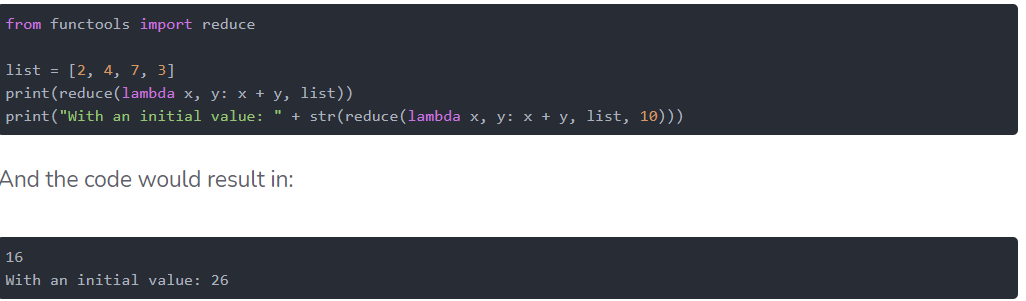
The **map()** function iterates through all items in the given iterable and executes the function we passed as an argument on each of them.



Similar to map(), **filter()** takes a function object and an iterable and creates a new list.

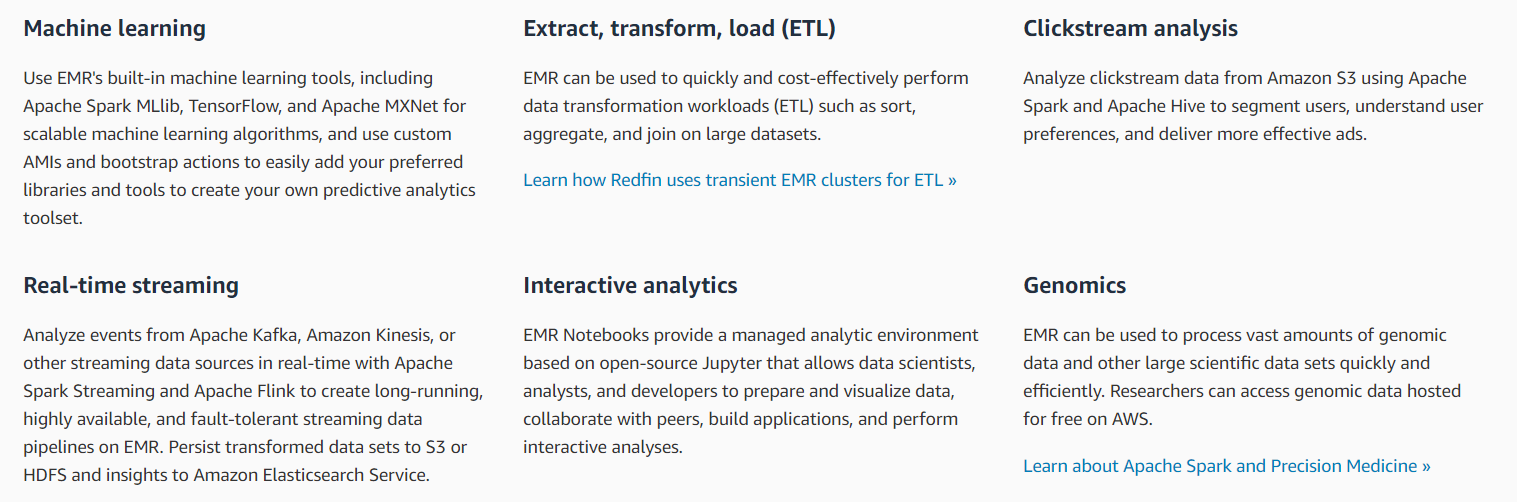


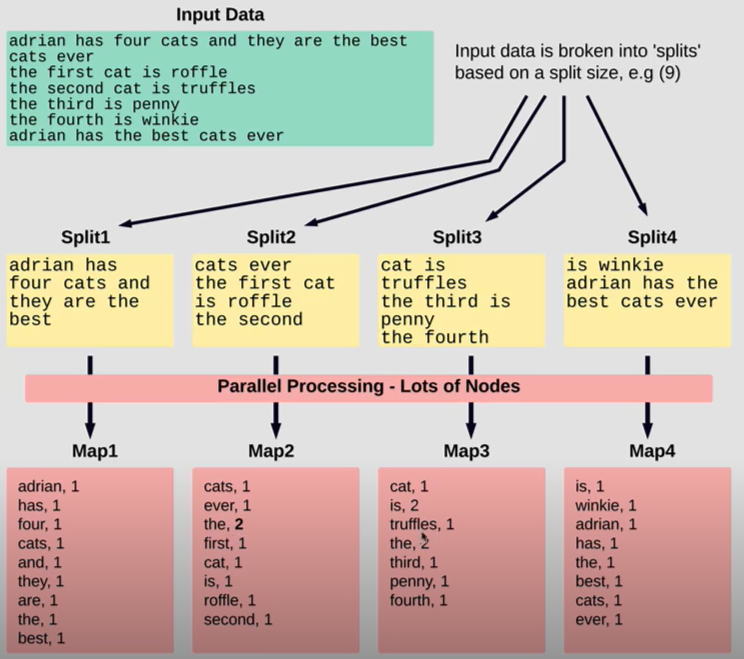
**reduce()** works differently than map() and filter(). It does not return a new list based on the function and iterable we've passed. Instead, it returns a single value.

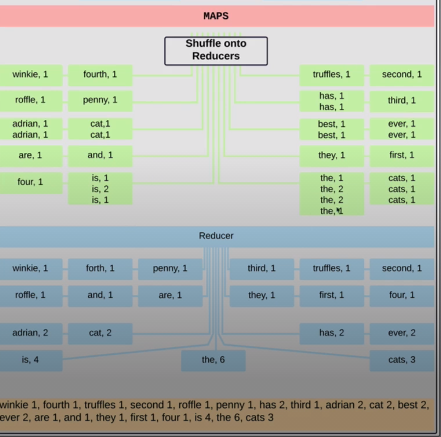


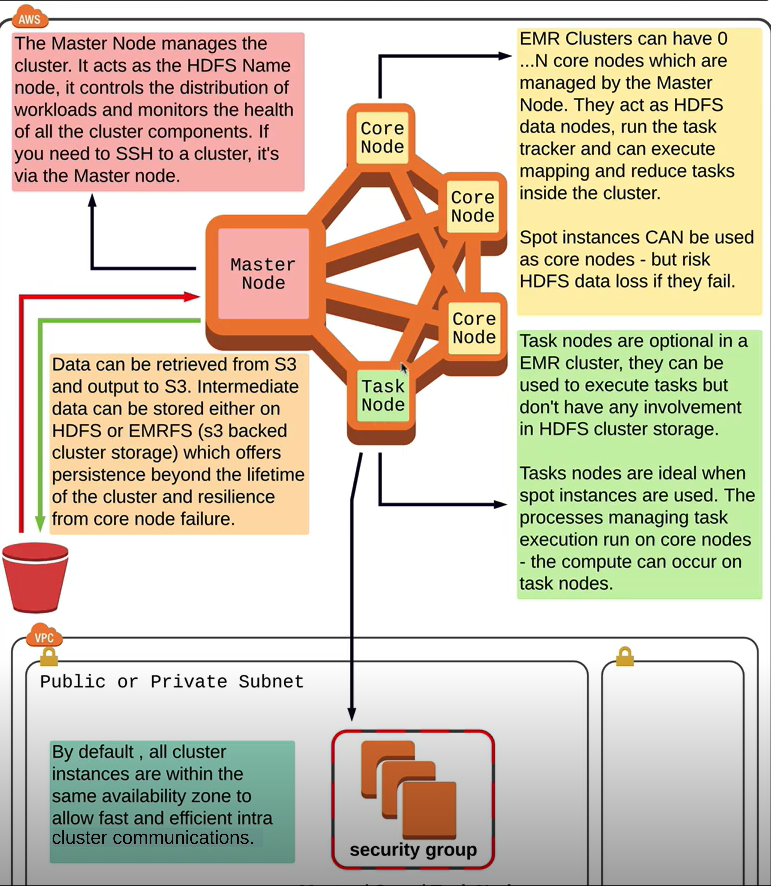
EMR – suitable for large amunts of data (TB, PB) which can be modularized and you need to perform a basic operation on each of them. (billing).

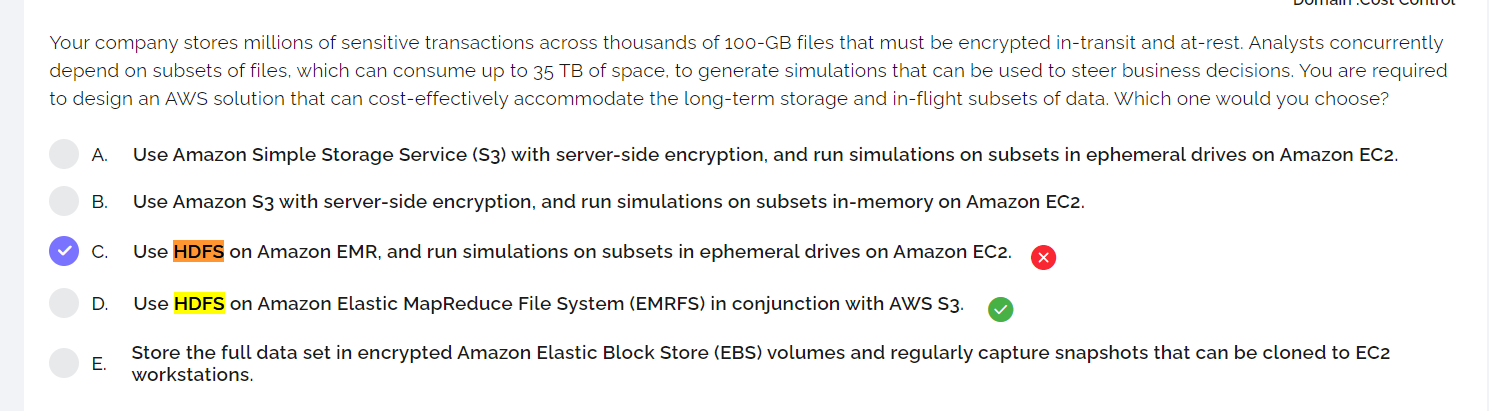
Combine EMR (input and output dataset) with peristent storage – s3.



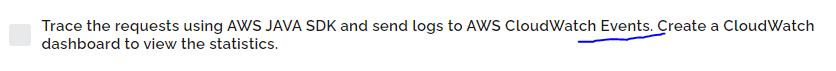


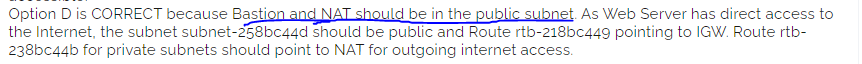




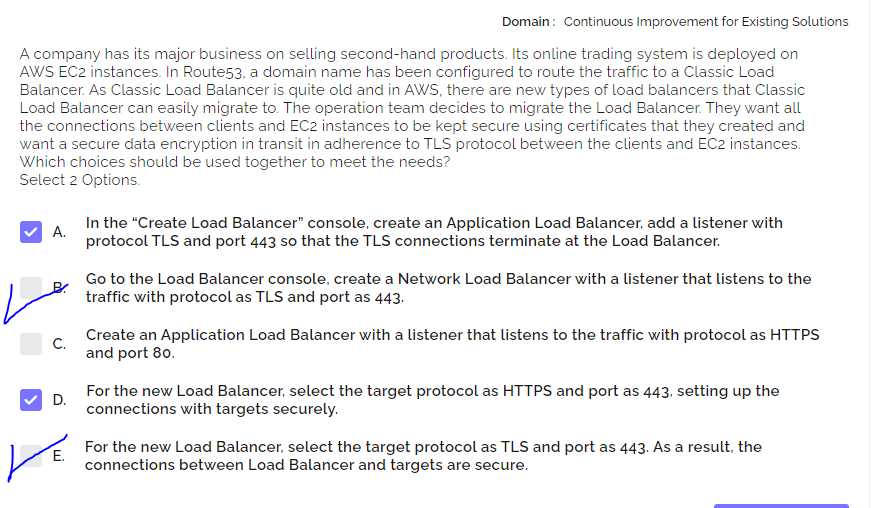


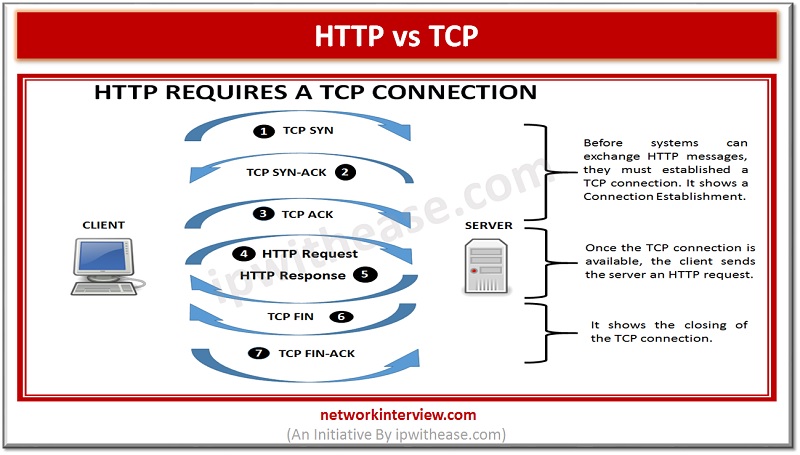
* 1. EC2Launch v2, EC2Launch, EC2Config
* EC2Launch v2 is a service that performs tasks during instance startup and runs if an instance is stopped and later started, or restarted.
* EC2Launch is a set of Windows PowerShell scripts that replaced the EC2Config service on Windows Server 2016 and later AMIs. The latest launch service for all supported Windows Server versions is EC2Launch v2, which replaces both EC2Config and EC2Launch.
* C2Config starts when the instance boots and performs tasks during startup and each time you stop or start the instance. EC2Config can also perform tasks on demand.
  1. The question tricks to fool you

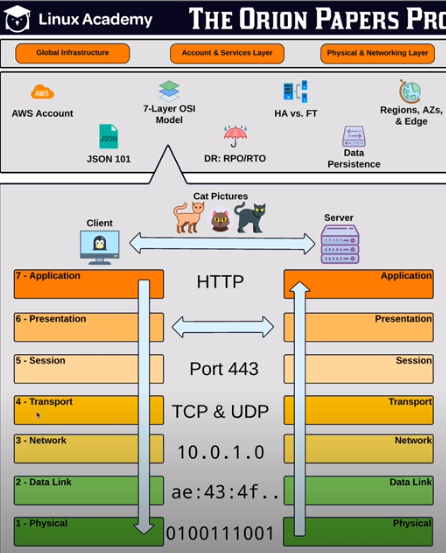


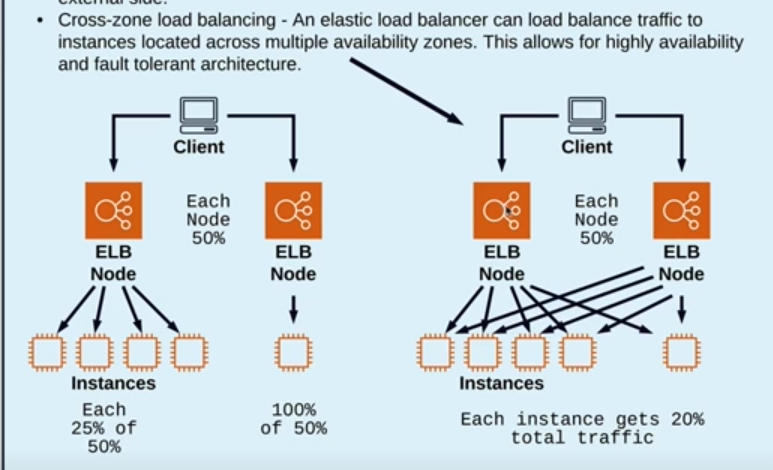


1. Whizlabs practice test 3
   1. Load Balancers









In newer versions of load balancers, the **cross zone load balancing** is enabled by default.

Elb has its own **dns record set** (A record), that allows access from its external site. You do not assign public Ips to load balancers, communication is based on CNAME.

Public facing vs internal

In case of the **public** facing LB each of the **nodes** (in azs ) get **public** **ips**.

The resource must be registered, either directly or indirectly (manually, auto scaling group, target group concept)

Difference between **“Load Balancer”** and **“Application” Generated Cookie Stickiness**

* Both options are going to rely on HTTP cookies to make sure that each session continues to hit the same instance.
* However, with option 2 (Load Balancer Generated Cookie), the EC2 load balancer will insert it's own cookie into the HTTP transaction with a specified expiration period. With Option 3 (Application Generated Cookie), you can have the load balancer check for cookies that you are already creating with your web app (like a PHP session ID) and the expiration period of the load balancer cookie will match that one.
* With the 3rd option, you have some control over how the cookie expires allowing the session to move to a different instance, but with the 2nd option, your application doesn't need to be creating any cookies.

**SSL Offloading**

* LB gets a certificate, does the encryption decrpytion. Gets https traffic from the public facing site and sends HTTP towards the target group.
* The data is not fully encrypted in transit, but u save some performance + its enoguh to manage just 1 certificate.

Load balancers decouple the tiers in the application and provide scalability / high availability.

* + 1. Classic

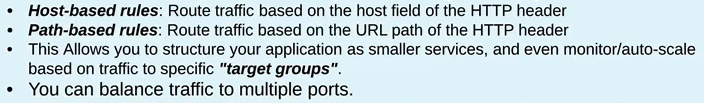
Classic load balancers dont understand layer 7 traffic. That means, that the only configuration granularity is listener configurations. I can only have a single listener (no prot based – L5, no path based L7)

Application LB by default in VPC

Netowrk LB if you have specific requirements

Classic LB only if you use Ec2 classic (what is that?!)

* + 1. Application LB



* Multiple certificates,
* both ipv4 and ipv6.
* Listener Protocols: HTTP / HTTPS.
* Security groups
* Target groups – no more direct association like in case of Classic LB
* Target types: Lambda IP, Target gruop
* For health checks multiple success codes are allowed
* ELB health checks are better then ec2
* Application load balancer can be used for more applications
* Authentication – you can validate request against a web identity
  + 1. Network LB
* You can configure static ip address for the newtwork lb
* Extreme performance
  + 1. E2E Encryption

Application LB

* It is not a single unbroken connection between client and the load balancer. If you have a listener on port 443 and forward traffic to the target group on port 80 (you did offloading) the 2nd traffic wont be encrypted. NOT a single unbroken connection between clients and the resources.

Network LB

* Since it does not support anything higher than layer 4 it does not interact with the encryption in any ways.
* Uninterrupted end to end encryption: Network load balancer
* Custom TCP protocols: you need to use NLB
* Does not support UDP
* Can route traffic outside to vpc.
  1. Cloudtrail

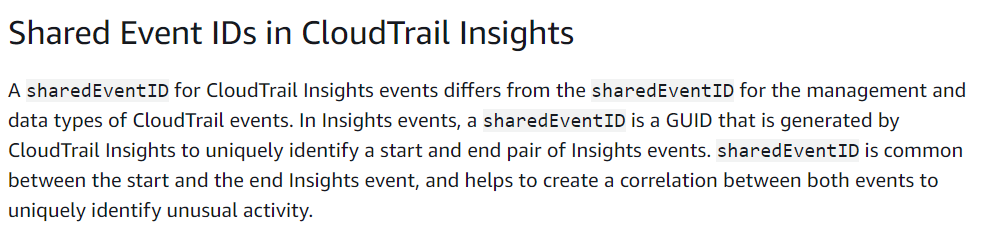
By default all api calls are recoded for 90 days.

The event might have been generated by you (iam user), by assuming a role or an aws service (lambda) made actions on your behalf.

Region: keep in mind trails can have duplicated data. Us-east-1 is the region for global events (iam)

In addition cloudtrail is capable of logging:

* Management events
* Data events



Enable log file validation – hashes, and validation files. You cannot move the files later on, the s3 bucket you set must be the final destincation. (Cloudtrail-Digest folder)