aws.amazon.com.

.com - Top-Level Domain (TLD)  (DOMAIN)

amazon - Second-Level Domain (SLD).

www and aws - any number of lower levels below the SLD.

Amazon Route 53 is an authoritative DNS system. An authoritative DNS system provides an update mechanism that developers use to manage their public DNS names.

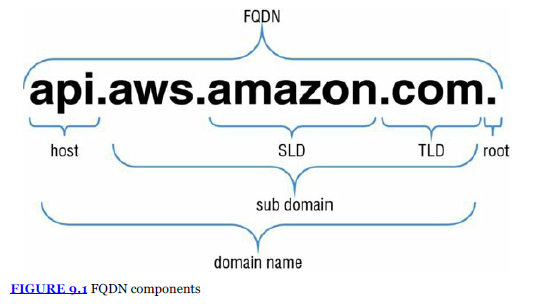
Certain parties are given management control over TLDs by the Internet Corporation for Assigned Names and Numbers (ICANN).

These parties can then distribute domain names under the TLD, usually through a domain registrar.

These domains are registered with the Network Information Center (InterNIC) - enforces the uniqueness of domain names across the Internet.

Domain Name – Example amazon.com (Subdomain)

left-most portions of a domain are the most specific. This is how DNS works: from most to least specific as you read from left to right.



**Name Servers – Multiple Name servers under a DNS**

A *name server* is a computer designated to translate domain names into IP addresses

**Zone Files**

A *zone file* is a simple text file that contains the mappings between domain names and IP addresses.

Zone files are the way that name servers store information about the domains they know.

A zone file describes a **DNS zone**, which is a subset of the entire DNS.

Zone files are generally used to configure a single domain,

$ORIGIN directive is a parameter equal to the zone’s highest level of authority by default. If a zone file is used to configure the example.com domain, the $ORIGIN would be set to example.com

$TTL directive configures the default Time to Live (TTL) value for resource records in the zone. This value defines the length of time that previously queried results are available to a caching name server before they expire.

A **domain name registrar** is an organization or commercial entity that manages the reservation of Internet domain names.

Domain Name

* Zone

(Zone file)

* Records
  + SOA
  + A or AAAA

DNS resolution

**Record Types**

Each zone file contains records. In its simplest form, a *record* is a single mapping between a resource and a name.

These can map a domain name to an IP address or define resources for the domain, such as name servers or mail servers

**Start of Authority (SOA) Record**

A *Start of Authority (SOA) record* is mandatory in all zone files, and it identifies the base DNS information about the domain. Each zone contains a single SOA record

* DNS server Name for the zone
* zone administrator
* default TTL
* some timeouts..

**A and AAAA**

map a host to an IP address.

A – for IPv4

AAAA – Ipv6 addresses

**Canonical Name (CNAME)**

defines an alias for the CNAME for your server

**Mail Exchange (MX)**

*Mail Exchange (MX) record*s are used to define the mail servers used for a domain and ensure that email messages are routed correctly.

The MX record should point to a host defined by an A or AAAA record and not one defined by a CNAME

**Name Server (NS)**

*Name Server (NS) record*s are used by TLD servers to direct traffic to the DNS server that contains the authoritative DNS records.

**Pointer (PTR)**

PTR records map an IP address to a DNS name,

used to check if the server name is associated with the IP address from where the connection was initiated.

**Text (TXT)**

to hold text information.

ability to associate some arbitrary and unformatted text with a host or other name, such as human readable information about a server, network, data center, and other accounting information.

**Service (SRV)**

a specification of data in the DNS defining the location (the host name and port number) of servers for specified services.

Service example – web/http

**Sender Policy Framework (SPF)**

S*ender Policy Framework (SPF) record*s are used by mail servers to combat spam. An SPF record tells a mail server what IP addresses are authorized to send an email from your domain name.

This prevents people from spoofing emails from your domain name.

Amazon Route 53 performs three main functions:

***Domain registration***

option to transfer the domain registration to Amazon Route 53.

***DNS service***—

If you register a new domain name with Amazon Route 53, Amazon Route 53 will be automatically configured as the DNS service for the domain,

*hosted zone* will be created for your domain.

You add resource record sets to the hosted zone, which define how you want Amazon Route 53 to respond to DNS queries for your domain

If you’re using Amazon CloudFront, Amazon Simple Storage Service (Amazon S3), or Elastic Load Balancing, you can configure Amazon Route 53 to route Internet traffic to those resources

***Health checking***—

**Hosted Zones**

A *hosted zone* is a collection of resource record sets hosted by Amazon Route 53.

Like a traditional DNS zone file, a hosted zone represents resource record sets that are managed together under a single domain name

A private hosted zone*-* how you want to route traffic for a domain and its subdomains within one or more Amazon Virtual Private Clouds (Amazon VPCs)

A *public hosted zone – internet traffic*

The resource record sets contained in a hosted zone must share the same suffix. For example, the example.com hosted zone can contain resource record sets for the [www.example.com](http://www.example.com) and [www.aws.example.com](http://www.aws.example.com) subdomains, but it cannot contain resource record sets for a [www.example.ca](http://www.example.ca) subdomain.

Use an alias record, not a CNAME, for your hosted zone. CNAMEs are not allowed for hosted zones in Amazon Route 53.

Do not use A records for subdomains (for example, [www.domain.com](http://www.domain.com)), as they refer to hardcoded IP addresses. Instead, use Amazon Route 53 alias records or traditional CNAME records to always point to the right resource, wherever your site is hosted, even when the physical server has changed its IP address.

**Supported Record Types**

Supported record types include:

A

AAAA

CNAME

MX

NS

PTR

SOA

SPF

SRV

TXT

Routing Policies

**Simple**

Use it when there is only web server

**Weighted**

2 webservers – across region or within region

Assign weight, distribute traffic accordingly

Possibility = weight/total weight

Example : 10 % to test new version of website, remaining 90% to prod env..

**Latency-Based**

*Latency-based routing* allows you to route your traffic based on the lowest network latency for your end user

**Failover**

Use a failover routing policy to configure active-passive failover, in which one resource takes all the traffic when it’s available and the other resource takes all the traffic when the first resource isn’t available.

Only for public and not private hosted zones

Amazon Route 53 will monitor the health of your primary resource endpoints using a health check

A health check tells Amazon Route 53 how to send requests to the endpoint whose health you want to check: which protocol to use (HTTP, HTTPS, or TCP), which IP address and

port to use, and, for HTTP/HTTPS health checks, a domain name and path.

After you have configured a health check, Amazon will monitor the health of your selected DNS endpoint. If your health check fails, then failover routing policies will be applied and your DNS will fail over to your DR site.

**Geolocation**

*Geolocation routing* lets you choose where Amazon Route 53 will send your traffic based on the geographic location of your users

You can specify geographic locations by continent, by country, or even by state in the United States.

You can also create separate resource record sets for overlapping geographic regions, and priority goes to the smallest geographic region

One record set for EU and one for UK, priority for UK..

What about IPS that are not mapped to a given region/country/state

In this case, you can **create a default resource record** set that handles both queries from IP addresses that aren’t mapped to any location and queries that come from locations for which you haven’t created geolocation resource record sets.

If you don’t create a default resource record set, Amazon Route 53 returns a “no answer” response for queries from those locations

You cannot create two geolocation resource record sets that specify the same geographic location.

You also cannot create geolocation resource record sets that have the same values for “Name” and “Type” as the “Name” and “Type” of non-geolocation resource record sets.

Amazon Route 53 health checks are not triggered by DNS queries; they are run periodically by AWS, and results are published to all DNS servers. This way, name servers

can be aware of an unhealthy endpoint and route differently within approximately 30 seconds of a problem (after three failed tests in a row), and new DNS results will be

known to clients a minute later (assuming your TTL is 60 seconds), bringing complete recovery time to about a minute and a half in total in this scenario.

**D. DNS primarily uses UDP to serve requests.**

**A. The TCP protocol is used by DNS server when the response data size exceeds 512 bytes or for tasks such as zone transfers.**

1 - c

2 - B

3  C

4 D

5 B

6 C

7 B

8 B

9 D

10 D

1 B

2 C

3 A

4 C

5 B

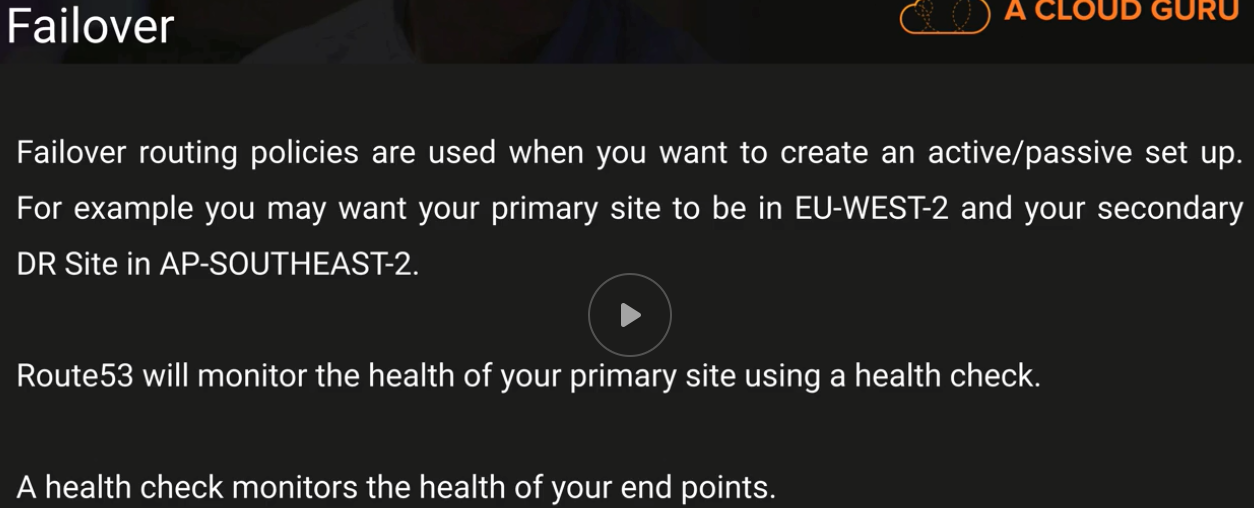
6 B D

7  C A

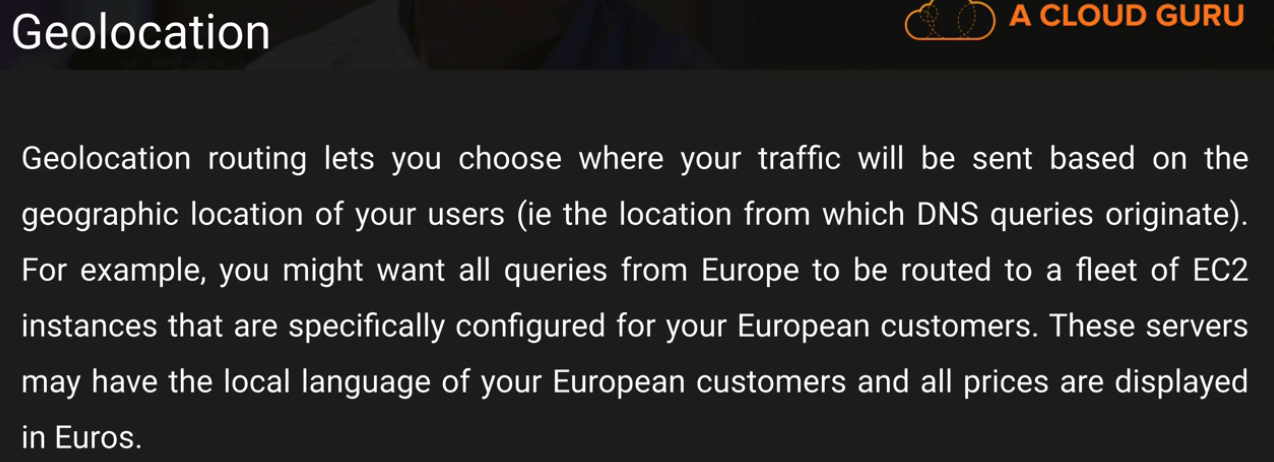
8  B

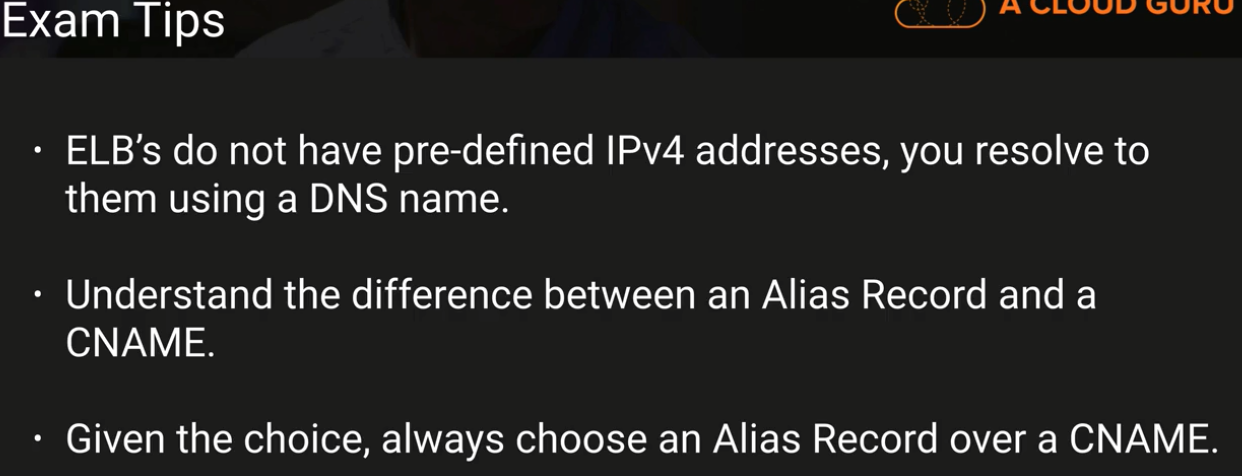
9 D

10 A D



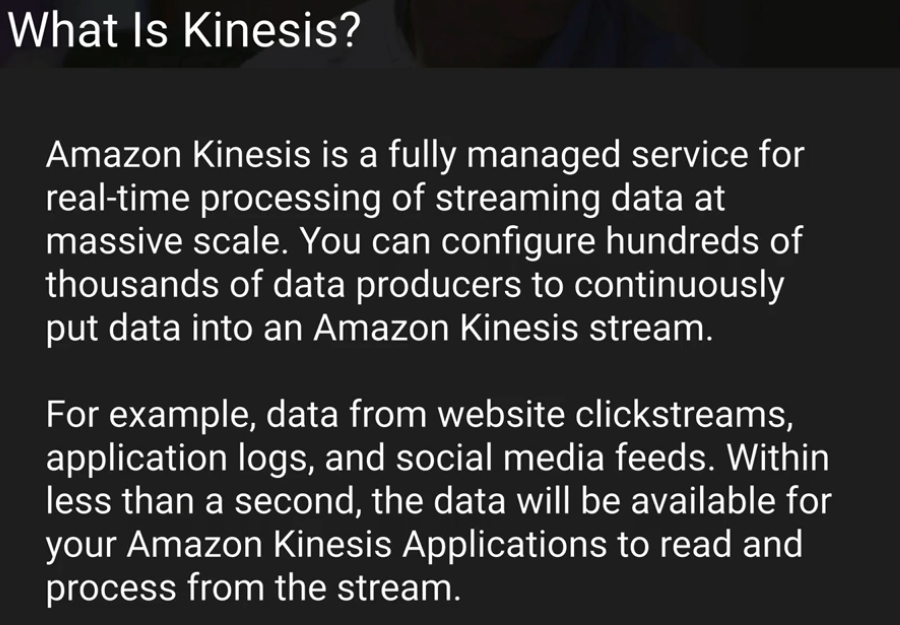


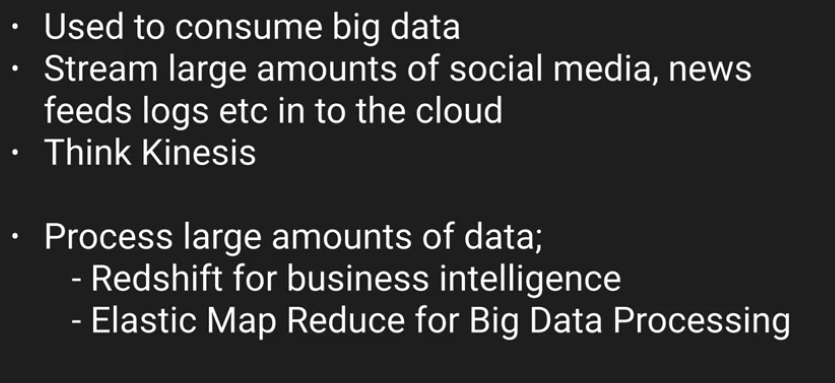


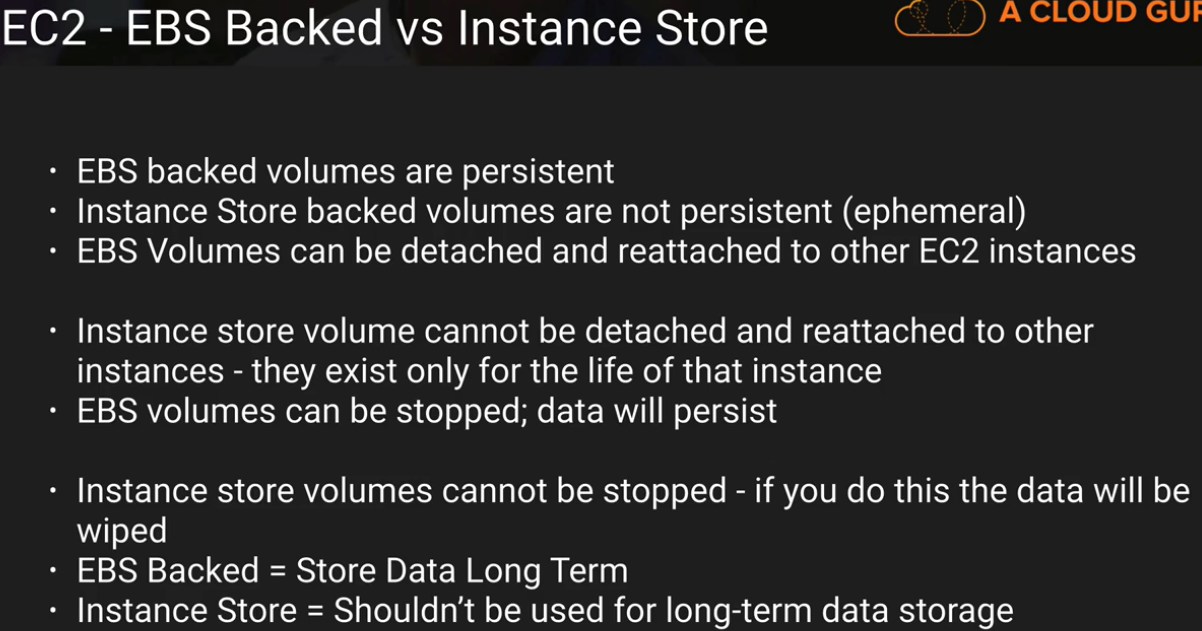


Exam Tips

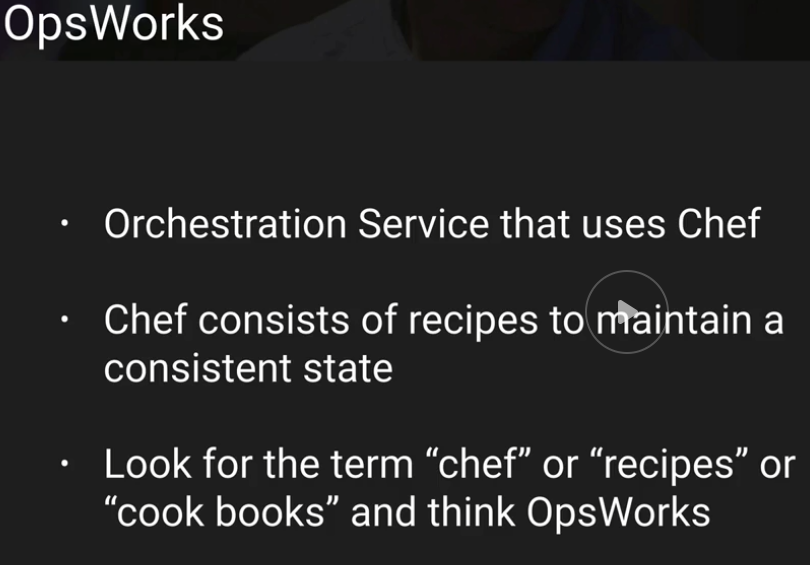
Questions – Way to consume data  Kinesis

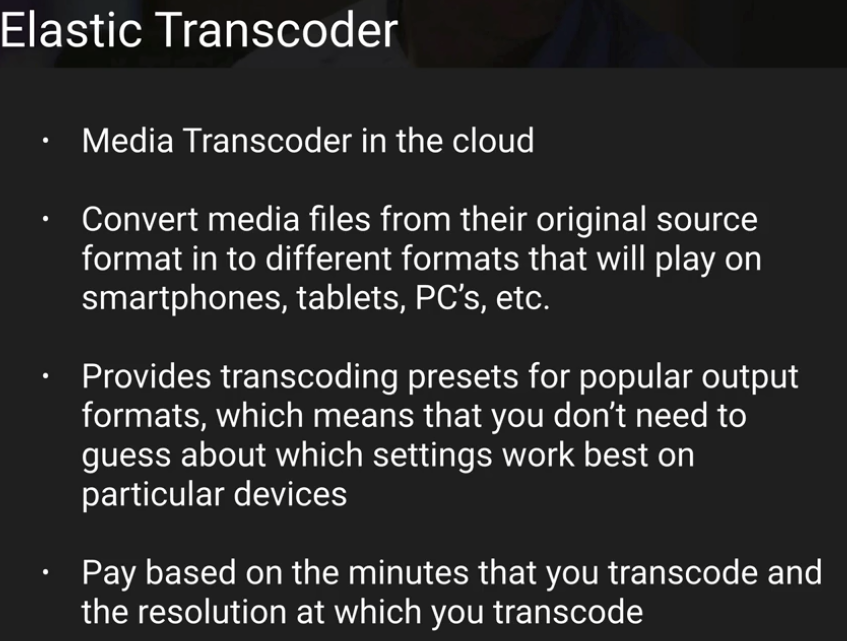


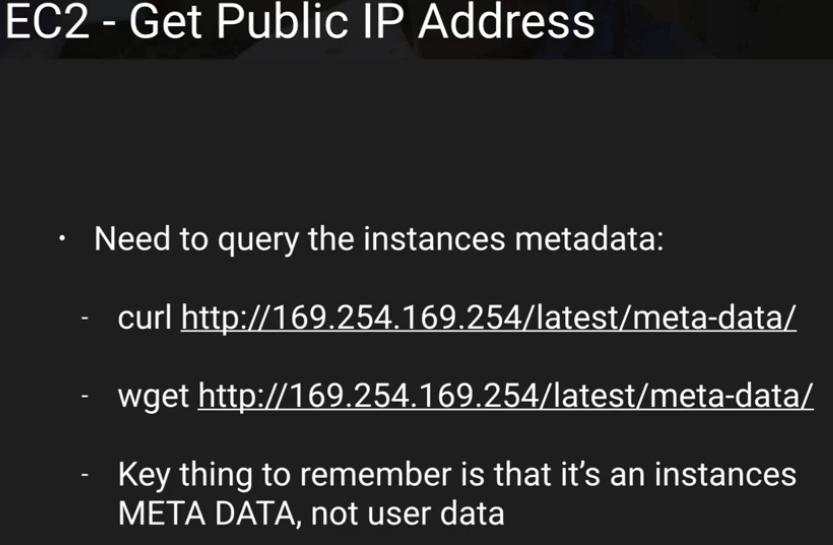




**OpsWorks**







Thanks & Regards,

Shantaram Vernekar