AWS Solution Architect Associate Certification Training – Module 15

15. Route53

What is Amazon Route 53?

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.

Amazon Route 53 effectively connects user requests to infrastructure running in AWS – such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets – and can also be used to route users to infrastructure outside of AWS. You can use Amazon Route 53 to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of your application and its endpoints.

Features

- Highly available and reliable
- Flexible
- Designed for use with other Amazon Web Services
- Simple
- Fast
- Cost-effective
- Secure
- Scalable
- Simplify the hybrid cloud

How DNS Works

DNS is a global system for translating IP addresses to human-readable domain names. When a user tries to access a web address like "example.com", their web browser or application performs a DNS Query against a DNS server, supplying the hostname. The DNS server takes the hostname and resolves it into a numeric IP address, which the web browser can connect to.

A component called a DNS Resolver is responsible for checking if the hostname is available in local cache, and if not, contacts a series of DNS Name Servers, until eventually it receives the IP of the service the user is trying to reach, and returns it to the browser or application. This usually takes less than a second.

Types or classification of Domains

DNS Types: 3 DNS Query Types

There are three types of queries in the DNS system:

Recursive Query:

In a recursive query, a DNS client provides a hostname, and the DNS Resolver "must" provide an answer—it responds with either a relevant resource record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS Root Server, until it finds the Authoritative Name Server (for more on Authoritative Name Servers see DNS Server Types below) that holds the IP address and other information for the requested hostname.

Iterative Query:

In an iterative query, a DNS client provides a hostname, and the DNS Resolver returns the best answer it can. If the DNS resolver has the relevant DNS records in its cache, it returns them. If not, it refers the DNS client to the Root Server, or another Authoritative Name Server which is nearest to the required DNS zone. The DNS client must then repeat the query directly against the DNS server it was referred to.

Non-Recursive Query:

A non-recursive query is a query in which the DNS Resolver already knows the answer. It either immediately returns a DNS record because it already stores it in local cache, or queries a DNS Name Server which is authoritative for the record, meaning it definitely holds the correct IP for that hostname. In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client.

DNS Types: 3 Types of DNS Servers

The following are the most common DNS server types that are used to resolve hostnames into IP addresses.

DNS Resolver:

A DNS resolver (recursive resolver), is designed to receive DNS queries, which include a human-readable hostname such as "www.example.com", and is responsible for tracking the IP address for that hostname.

DNS Root Server:

The root server is the first step in the journey from hostname to IP address. The DNS Root Server extracts the Top Level Domain (TLD) from the user's query—for example, www.example.**com**—and provides details for the **.com** TLD Name Server. In turn, that server will provide details for domains with the .com DNS zone, including "example.com".

Authoritative DNS Server:

Higher level servers in the DNS hierarchy define which DNS server is the "authoritative" name server for a specific hostname, meaning that it holds the up-to-date information for that hostname.

The Authoritative Name Server is the last stop in the name server query—it takes the hostname and returns the correct IP address to the DNS Resolver (or if it cannot find the domain, returns the message NXDOMAIN).

Domain registration, Domain Hosting and Domain transfer

Domain registration

When you want to get a new domain name, such as the **example.com** part of the URL http://example.com, you can register it with Amazon Route 53. You can also transfer the registration for existing domains from other registrars to Route 53 or transfer the registration for domains that you register with Route 53 to another registrar.

Domain Hosting

Domain hosting refers to businesses that specialize in hosting domain names for individuals and companies. Domain names are used in URLs to identify particular Web pages.

Domain transfer

A domain transfer refers to the process of changing the designated registrar of a domain name. ... Domain names may be transferred only if they have been registered with the previous registrar for 60 days or more .

Public and Private hosted zones

A hosted zone is a container for records, and records contain information about how you want to route traffic for a specific domain, such as example.com, and its subdomains (acme.example.com, zenith.example.com). A hosted zone and the corresponding domain have the same name. There are two types of hosted zones:

Public hosted zone:

A public hosted zone is a container that holds information about how you want to route traffic on the internet for a specific domain, such as example.com, and its subdomains (acme.example.com, zenith.example.com). You get a public hosted zone in one of two ways:

- When you register a domain with Route 53, we create a hosted zone for you automatically.

- When you transfer DNS service for an existing domain to Route 53, you start by creating a hosted zone for the domain.

Private hosted zone:

A *private hosted zone* is a container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains within one or more VPCs that you create with the Amazon VPC service.

Here's how private hosted zones work:

1. You create a private hosted zone, such as example.com, and specify the VPCs that you want to associate with the hosted zone.

2. You create records in the hosted zone that determine how Route 53 responds to DNS queries for your domain and subdomains within and among your VPCs. For example, suppose you have a database server that runs on an EC2 instance in one of the VPCs that you associated with your

private hosted zone. You create an A or AAAA record, such as db.example.com, and you specify the IP address of the database server.

3. When an application submits a DNS query for db.example.com, Route 53 returns the corresponding IP address. The application must also be running on an EC2 instance in one of the VPCs that you associated with the example.com private hosted zone.

4. The application uses the IP address that it got from Route 53 to establish a connection with the database server.

Health check of Resources

Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. Each health check that you create can monitor one of the following:

- The health of a specified resource, such as a web server

- The status of other health checks

- The status of an Amazon CloudWatch alarm