Amazon Route53

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 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

Amazon Route53 Capabilities

Amazon Route 53 Provides below services:

- Domain registration
- DNS management
- Traffic management
- Availability monitoring

Domain registration

Register New Domain Name

- 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.

Transfer Existing Domain Name

- You can also transfer the registration for existing domains from other registrars to Amazon Route 53 or transfer the registration for domains that you register with Amazon Route 53 to another registrar

Domain registration

- When you register a domain with Amazon Route 53 or you transfer domain registration to Amazon Route 53, we configure the domain to renew automatically. The automatic renewal period is typically one year, although the registries for some top-level domains (TLDs) have longer renewal periods.

- Registries for top-level domains (such as .com) have requirements for transferring domains. Requirements vary among TLDs, but the following requirements are typical:
  - You must have registered the domain with the current registrar at least 60 days ago.
  - If the registration for a domain name expired and had to be restored, it must have been restored at least 60 days ago.
  - You must have transferred registration for the domain to the current registrar at least 60 days ago.
  - The domain cannot have any of the following domain name status codes:
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - clientTransferProhibited
  - Some registries block transfers until changes, such as ownership changes, are complete.

DNS Service

- Route53 provides Hosted DNS Service

- Create a hosted zone that can store DNS records for your domain. Upon creating the hosted zone, you receive four Route 53 name servers across four different Top-Level Domains (TLDs) to help ensure a high level of availability.

- Your hosted zone will be initially populated with a basic set of DNS records, including four virtual name servers that will answer queries for your domain.

DNS Service

- Amazon Route 53 currently supports the following DNS record types:
  - A (address record)
  - AAAA (IPv6 address record)
  - CNAME (canonical name record)
  - MX (mail exchange record)
  - NS (name server record)
  - PTR (pointer record)
  - SOA (start of authority record)
  - SPF (sender policy framework)
  - SRV (service locator)
  - TXT (text record)
  - Additionally, Route 53 offers 'Alias' records (a Route 53-specific virtual record).

DNS Service

Option 1

- Whenever you register a Domain name or transfer domain with Route53 It automatically create a Hosted DNS service for that domain

Option 2

- Keep the domain name with Registrar, inform the registrar to update the name servers for your domain to the ones associated with your hosted zone.

Option 3:

- Creating a Subdomain That Uses Amazon Route 53 as the DNS Service without Migrating the Parent Domain

Option 4:

You can migrate a subdomain to use Amazon Route 53 as the DNS service without migrating the parent domain from another DNS service.

DNS management

- Routing Queries to a Cloud Front distribution
- Routing Queries to an Elastic Load Balancing Load Balancer (Public Hosted Zones Only)
- Routing Queries to an Amazon EC2 Instance
- Routing Queries to a Website That Is Hosted in an Amazon S3 Bucket (Public Hosted Zones Only)
- Routing Queries to an Amazon Relational Database Service (Amazon RDS) Database
- Routing Queries to Amazon WorkMail (Public Hosted Zones Only)

Private Hosted Zones

- A public hosted zone is a container that holds information about how you want to route traffic on the Internet for a domain, such as example.com, and its subdomains (apex.example.com, acme.example.com).

- After you create a public hosted zone, you create resource record sets that determine how the Domain Name System (DNS) responds to queries for your domain and subdomains.

Private Hosted Zones

- A private hosted zone is a container that holds information about how you want to route traffic for a domain and its subdomains within one or more Amazon Virtual Private Clouds (Amazon VPCs).

- To begin, you create a private hosted zone and specify the Amazon VPCs that you want to associate with the hosted zone.

- You then create resource record sets that determine how Amazon Route 53 responds to queries for your domain and subdomains within and among your Amazon VPCs.

split-view DNS

- You can use Amazon Route 53 to configure split-view DNS, also known as split-horizon DNS.

- If you want to maintain internal and external versions of the same website or application (for example, for testing changes before you make them public), you can configure public and private hosted zones to return different internal and external IP addresses for the same domain name.

- Just create a public hosted zone and a private hosted zone that have the same domain name, and create the same subdomains in both hosted zones.

- When you have private and public hosted zones, the private hosted zone takes precedence over the public hosted zone when you're logged into an Amazon EC2 instance in an Amazon VPC that you have associated with the private hosted zone.

- To use private hosted zones, you must set the following Amazon VPC settings to`true`:
  - `enableDnsHostnames`
  - `enableDnsSupport`

Traffic management

Routing Policy

- When you create a resource record set, you choose a routing policy, which determines how Amazon Route 53 responds to queries:
  - **Simple Routing Policy**
  - **Weighted Routing Policy**
  - **Latency Routing Policy**
  - **Failover Routing Policy (Public Hosted Zones Only)**
  - **Geolocation Routing Policy**

Simple Routing Policy

- Use a simple routing policy when you have a single resource that performs a given function for your domain, for example, one web server that serves content for the example.com website.

- In this case, Amazon Route 53 responds to DNS queries based only on the values in the resource record set, for example, the IP address in an A record.

Weighted Routing Policy

- Use the weighted routing policy when you have multiple resources that perform the same function

- for example, web servers that serve the same website and you want Amazon Route 53 to route traffic to those resources in proportions that you specify (for example, one quarter to one server and three quarters to the other).

Latency Routing Policy

Map courtesy of the University of Texas Libraries, The University of Texas at Austin.

- Use the latency routing policy when you have resources in multiple Amazon EC2 data centers that perform the same function and you want Amazon Route 53 to respond to DNS queries with the resources that provide the best latency.

- For example, you might have web servers for example.com in the Amazon EC2 data centers in Ireland and in Tokyo. When a user browses to example.com, Amazon Route 53 chooses to respond to the DNS query based on which data center gives your user the lowest latency.

Geolocation Routing

- Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location from which DNS queries originate.

- For example, you might want all queries from Africa to be routed to a web server with an IP address of 192.0.2.111.

- When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights.

- Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.

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

Traffic Flow to Route DNS Traffic

- Amazon Route 53 traffic flow provides a visual editor that helps you create complex trees in a fraction of the time with a fraction of the effort.

- You can save the configuration as a *traffic policy* and then associate the traffic policy with one or more domain names (such as example.com) or subdomain names (such as www.example.com), in the same hosted zone or in multiple hosted zones.

- You can also use the visual editor to quickly find resources that you need to update and apply the updates to one or more DNS names such as www.example.com.

- In addition, you can roll back the updates if the new configuration isn't performing as you expected it to.

Availability monitoring

Availability monitoring

- Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. At regular intervals that you specify, Amazon Route 53 submits automated requests over the Internet to your application, server, or other resource to verify that it's reachable, available and functional.

- You can configure a health check to make requests similar to those that your users make, such as:
  - requesting a web page from a specific URL.
  - view the current and recent status of health checks
  - receive a notification when an application or a resource becomes unavailable
  - configure an Amazon CloudWatch alarm for each health check.

- If you have multiple resources that perform the same function, for example, web servers or email servers, and you want Amazon Route 53 to route traffic only to the resources that are healthy, you can configure DNS failover by associating health checks with your resource record sets. If a health check determines that the underlying resource is unhealthy, Amazon Route 53 routes traffic away from the associated resource record set.

Configuring DNS Failover

- **Active-active failover:** Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Amazon Route 53 can detect that it's unhealthy and stop including it when responding to queries.

- **Active-passive failover:** Use this failover configuration when you want a primary group of resources to be available the majority of the time and you want a secondary group of resources to be on standby in case all of the primary resources become unavailable. When responding to queries, Amazon Route 53 includes only the healthy primary resources. If all of the primary resources are unhealthy, Amazon Route 53 begins to include only the healthy secondary resources in response to DNS queries.

- **Active-active-passive and other mixed configurations:** You can combine alias and non-alias resource record sets to produce a variety of Amazon Route 53 behaviors

Alias and Non-Alias Resource Record Sets

- While ordinary Amazon Route 53 resource record sets are standard DNS resource record sets, *alias resource record sets* provide an Amazon Route 53–specific extension to DNS functionality.

- Instead of an IP address or a domain name, an alias resource record set contains a pointer to a CloudFront distribution, an ELB load balancer, an Amazon S3 bucket that is configured as a static website, or another Amazon Route 53 resource record set in the same hosted zone.

- When Amazon Route 53 receives a DNS query that matches the name and type in an alias resource record set, Amazon Route 53 follows the pointer and responds with the applicable value:
  - **An alternate domain name for a CloudFront distribution:** Amazon Route 53 responds as if the query had asked for the CloudFront distribution by using the CloudFront domain name, such as d111111abcdef8.cloudfront.net.
  - **An ELB load balancer:** Amazon Route 53 responds to each request with one or more IP addresses for the load balancer.
  - **An Amazon S3 bucket that is configured as a static website:** Amazon Route 53 responds to each request with one IP address for the Amazon S3 bucket.
  - **Another Amazon Route 53 resource record set in the same hosted zone:** Amazon Route 53 responds as if the query had asked for the resource record set that is referenced by the pointer.

Alias and Non-Alias Resource Record Sets

- Alias resource record sets can save you time because Amazon Route 53 automatically recognizes changes in the resource record sets that the alias resource record set refers to.

- For example, suppose an alias resource record set for example.com points to an ELB load balancer at lb1-1234.us-east-1.elb.amazonaws.com. If the IP address of the load balancer changes, Amazon Route 53 will automatically reflect those changes in DNS answers for example.com without any changes to the hosted zone that contains resource record sets for example.com.

Alias and Non-Alias Resource Record Sets

CNAME Records	Alias Records
Amazon Route 53 charges for CNAME queries.	Amazon Route 53 doesn't charge for alias queries to CloudFront distributions, ELB load balancers, or Amazon S3 buckets. For more information, see Amazon Route 53 Pricing.
You cannot create a CNAME record at the top node of a DNS namespace, also known as the *zone apex*. For example, if you register the DNS name example.com, the zone apex is example.com.	You can create an alias resource record set at the zone apex.
A CNAME record redirects queries for a domain name regardless of record type.	Amazon Route 53 follows the pointer in an alias resource record set only when the record type also matches.
A CNAME record can point to any DNS record hosted anywhere, including to the resource record set that Amazon Route 53 automatically creates when you create a policy record. For more information, see Using Traffic Flow to Route DNS Traffic.	An alias resource record set can only point to a CloudFront distribution, an ELB load balancer, an Amazon S3 bucket that is configured as a static website, or another resource record set in the same Amazon Route 53 hosted zone in which you're creating the alias resource record set. However, you can't create an alias that points to the resource record set that Amazon Route 53 creates when you create a policy record.
A CNAME record is visible in the answer section of a reply from an Amazon Route 53 DNS server.	An alias resource record set is only visible in the Amazon Route 53 console or the Amazon Route 53 API.
A CNAME record is followed by a recursive resolver.	An alias resource record set is only followed inside Amazon Route 53. This means that both the alias resource record set and its target must exist in Amazon Route 53.

Demo