



Route 53

Hosted Zone: A container for DNS records that define how to route traffic for a specific domain or subdomain. There are two types:

- **Public Hosted Zone:** Routes traffic on the internet.
- **Private Hosted Zone:** Routes traffic within one or more VPCs (Virtual Private Clouds).

DNS Record Types: Different types of DNS records used to define how to route traffic for a domain. Common types include:

- **A (Address) Record:** Maps a domain or subdomain to an IPv4 address.
- **AAAA Record:** Maps a domain or subdomain to an IPv6 address.
- **CNAME (Canonical Name) Record:** Maps an alias name to a true or canonical domain name.
- **MX (Mail Exchange) Record:** Specifies the mail server responsible for receiving emails for a domain.
- **NS (Name Server) Record:** Specifies the authoritative name servers for a hosted zone.
- **SOA (Start of Authority) Record:** Provides information about the domain and the zone, including the primary name server and email of the domain administrator.
- **TXT (Text) Record:** Allows the domain owner to associate arbitrary text with a domain.

Alias Record: A Route 53-specific record type that is similar to a CNAME record, but it can be used for the root domain (e.g., example.com). Alias records are often used to map a domain name to an AWS resource like an Amazon S3 bucket or a CloudFront distribution.

Health Check: A feature that Route 53 uses to monitor the health of your resources. Health checks are performed periodically, and if a resource is unhealthy, Route 53 can route traffic away from it to healthy resources.



Route 53


Routing Policies: Determine how Route 53 responds to DNS queries. Common routing policies include:

- **Simple Routing:** Routes traffic to a single resource.
- **Weighted Routing:** Routes traffic based on weights assigned to different resources.
- **Latency-Based Routing:** Routes traffic to the resource with the lowest latency.
- **Failover Routing:** Routes traffic to a primary resource unless it is unhealthy, then routes to a secondary resource.
- **Geolocation Routing:** Routes traffic based on the geographic location of the user.
- **Geoproximity Routing:** Routes traffic based on the geographic location of the user and resource, with bias options.
- **Multi-Value Answer Routing:** Provides multiple IP addresses in response to DNS queries and performs health checks to only return healthy IP addresses.
- **TTL (Time to Live):** The amount of time in seconds that DNS resolvers should cache the DNS information before requesting a new one. A lower TTL results in more frequent updates but higher DNS query traffic.

Domain Name System (DNS): A hierarchical and decentralized naming system for computers, services, or other resources connected to the internet or a private network. It translates human-friendly domain names (like example.com) into IP addresses (like 192.0.2.1).

Intro Parameters

- Global Service
- AWS managed **Authoritative DNS** (customer can update the DNS records and have full control over the DNS)
- Also, a Domain Registrar (for registering domain names)
- Only AWS service which provides 100% availability SLA
- Affected by client's DNS caching (not suitable for Blue-Green Deployment if the client caches DNS queries)

 It is recommended to use DNS names or URLs instead of IPs wherever possible



Route 53

Hosted Zone

- A container for DNS records that define how to route traffic to a domain and its subdomains.
- Hosted zone is queried to get the IP address from the hostname
- Two types:
 - **Public Hosted Zone**
 - resolves public domain names
 - can be queried by anyone on the internet
 - **Private Hosted Zone**
 - resolves private domain names
 - can only be queried from within the VPC



Route 53

Record Types

- **A** - maps a hostname to IPv4
- **AAAA** - maps a hostname to IPv6
- **CNAME** - maps a hostname to another hostname
 - The target is a domain name which must have an A or AAAA record
 - **Cannot point to root domains (Zone Apex)** Ex: you can't create a CNAME record for example.com, but you can create for something.example.com
- **NS** (Name Servers) - controls how traffic is routed for a domain
- **Alias** - maps a hostname to an AWS resource
 - **AWS proprietary**
 - Can point to root (zone apex) and non-root domains
 - **Alias Record is of type A or AAAA** (IPv4 / IPv6)
 - Targets can be
 - Elastic Load Balancers
 - CloudFront Distributions
 - API Gateway
 - Elastic Beanstalk environments
 - S3 Websites
 - VPC Interface Endpoints
 - Global Accelerator
 - Route 53 record in the same hosted zone
 - **Target cannot be EC2**



Route 53

Routing Policies

Simple

- Route to one or more resources
- If multiple values are returned, client chooses one at random (client-side load balancing)
- **No health check** (if returning multiple resources, some of them might be unhealthy)

Weighted

- Route a fraction of request to multiple resources
- Health checks
- Use case: testing a new application version by sending a small amount of traffic
- Can be used for **Active-Active failover** strategy

Latency-based

- Redirect to the resource that has the lowest latency
- Health checks
- Can be used for **Active-Active failover** strategy

Failover

- Primary & Secondary Records (if the primary application is down, route to secondary application)
- Health check must be associated with the primary record
- Used for **Active-Passive failover** strategy

Geolocation

- Routing based on the client's location
- Should create a “Default” record (in case there's no match on location)
- Use cases: restrict content distribution & language preference



Route 53

Geoproximity

- Route traffic to your resources based on the proximity of clients to the resources
- Ability to shift more traffic to resources based on the defined bias.
 - To expand (bias: 1 to 99) → more traffic to the resource
 - To shrink (bias: -1 to -99) → less traffic to the resource
- Resources can be:
 - AWS resources (specify AWS region)
 - Non-AWS resources (specify Latitude and Longitude)
- Uses **Route 53 Traffic Flow**



Route 53

Multi-value

- Route traffic to multiple resources (max 8)
- Health Checks (only healthy resources will be returned)

Health Checks

- HTTP Health Checks are only for public resources
- Allows for Automated DNS Failover
- Three types:
 - **Monitor an endpoint** (application or other AWS resource)
 - Multiple **global health checkers** check the endpoint health
 - Must configure the application firewall to allow incoming requests from the IPs of Route 53 Health Checkers
 - Supported protocols: HTTP, HTTPS and TCP
 - **Monitor other health checks** (Calculated Health Checks)
 - Combine the results of multiple Health Checks into one (AND, OR, NOT)
 - Specify how many of the health checks need to pass to make the parent pass
 - Usage: perform maintenance to your website without causing all health checks to fail
 - **Monitor CloudWatch Alarms** (to perform health check on private resources)
 - Route 53 health checkers are outside the VPC. They can't access private endpoints in VPC or on-premises resources.
 - Create a CloudWatch Metric and associate a CloudWatch Alarm to it, then create a Health Check that checks the CW alarm.



Route 53

GoDaddy with Route 53

Use GoDaddy as registrar and Route 53 as DNS: Once we register a hostname at GoDaddy, we need to update the name servers (NS) of GoDaddy to match the name servers of a public hosted zone created in Route 53. This way, GoDaddy will use Route 53's DNS.

Scenario based Questions

<https://lisireddy.medium.com/aws-route-53-scenario-based-questions-856602714658>