AWS Route 53 – Full Detailed Notes

🔹 What is AWS Route 53?

Amazon Route 53 is a **highly available and scalable cloud Domain Name System (DNS) web service**. It is designed to:

- Route end users to Internet applications.
- Perform health checks.
- Register domain names.

It is named "Route 53" because DNS uses port 53.

🔹 Main Functions of Route 53

1. **Domain Registration**
    - You can register new domain names directly through Route 53.
    - It supports automatic domain renewal, WHOIS privacy, and DNSSEC.
2. **DNS Service**
    - Translates domain names (like example.com) into IP addresses.
    - Supports various DNS record types.
3. **Health Checking and Monitoring**
    - Route 53 can check the health of resources (e.g., web servers) and route traffic away from unhealthy endpoints.
4. **Routing Policy Management**
    - Route 53 allows sophisticated traffic flow policies based on different routing strategies (e.g., latency, geolocation).

🔹 Key Components of Route 53

Component	Description
Hosted Zone	A container for records that belong to a domain.
Record Set	Defines how you want to route traffic for the domain or subdomain.
DNS Records	E.g., A, AAAA, CNAME, MX, NS, SOA, TXT, etc.
Health Checks	Monitor the health of endpoints (IP or URL).
Routing Policies	Control traffic distribution strategies.

🔹 Types of DNS Records

Record Type	Description
A	Maps domain to an IPv4 address.
AAAA	Maps domain to an IPv6 address.
CNAME	Maps domain to another domain name.
MX	Mail exchange records for email servers.
NS	Nameserver records.
SOA	Start of Authority record – metadata about the domain.
TXT	Text records for domain verification (e.g., SPF, DKIM).
SRV	Service locator for services like SIP or LDAP.
CAA	Specifies which CAs are allowed to issue certificates.

🔹 Routing Policies

Policy Type	Description
Simple Routing	One record = one IP. No health checks.
Failover Routing	Routes traffic to healthy resources.
Geolocation Routing	Routes traffic based on the location of the user.
Geoproximity Routing	Routes traffic based on proximity using traffic bias (only in Traffic Flow).
Latency-based Routing	Sends user to the lowest latency region.
Multivalue Answer	Like simple routing but allows multiple IPs with health checks.
Weighted Routing	Assign weights to resources for load distribution.

🔹 Types of Hosted Zones

Type	Use Case
Public	Used for internet-facing DNS.
Private	Used within an Amazon VPC. Routes names only within VPC(s).

- **Health Checks**
  - Can monitor:
    - IP addresses (TCP, HTTP, HTTPS).
    - Web pages for keywords.
  - Integrates with **CloudWatch Alarms**.
  - You can set up **failover routing** based on health status.
  - You can **associate health checks with Route 53 records**.

- **Domain Registration with Route 53**
  - Can register and transfer domains (e.g., .com, .org, .io).
  - Provides WHOIS privacy for most domains.
  - Domains can be managed via AWS Management Console or CLI.

- **Security Features**
  - **DNSSEC (Domain Name System Security Extensions)** support for domain signing (only partial support).
  - Integrated with **IAM** for access control.
  - Supports **VPC Endpoint Policies** for private hosted zones.
  - Logging via **CloudTrail**.

- **Route 53 Traffic Flow (Advanced)**
  - GUI-based tool to manage traffic policies using visual editor.
  - Policies include:
    - Geoproximity
    - Weighted
    - Latency
    - Failover
  - Supports **versioning** and **policy rollback**.

- **Route 53 Resolver**

Used for:

- **DNS Resolution within VPC**.
- **Hybrid cloud setups** using **inbound and outbound endpoints**.
- **DNS forwarding** between on-premises and AWS.

Key Features:

- Outbound resolvers forward DNS queries to on-premises.
- Inbound resolvers allow on-premises networks to query AWS private DNS.

🔹 **Pricing Overview (as of 2024)**

Service	Price (Approx)
Hosted Zone	$0.50/month/zone
Standard Queries	$0.40 per million queries
Health Checks	$0.50/month per health check
Domain Registration	Varies by TLD (e.g., ~$12/year for .com)
Traffic Flow Policies	$50/month per policy
Resolver Endpoints	Charged per ENI hour

Note: Check AWS Pricing Calculator for the latest rates.

🔹 **Use Cases**

- Hosting scalable websites (e.g., S3 + CloudFront + Route 53).
- Disaster recovery with failover policies.
- Load balancing across regions.
- Global applications with latency-based routing.
- Hybrid cloud DNS using Resolver.

🔹 **Best Practices**

- Use TTLs wisely – short TTLs for frequently changing data.
- Enable health checks for high availability.
- Use private hosted zones for internal services.
- Secure domains with DNSSEC and WHOIS privacy.
- Use IAM policies to restrict access to DNS changes.