Amazon Route 53

Domain Name System

Content Prepared By: Chandra Lingam, Cotton Cola Designs LLC

amazon web services

Route 53

Highly available, Scalable, Globally Distributed Domain Name System (DNS) Service (IPv4, IPv6)

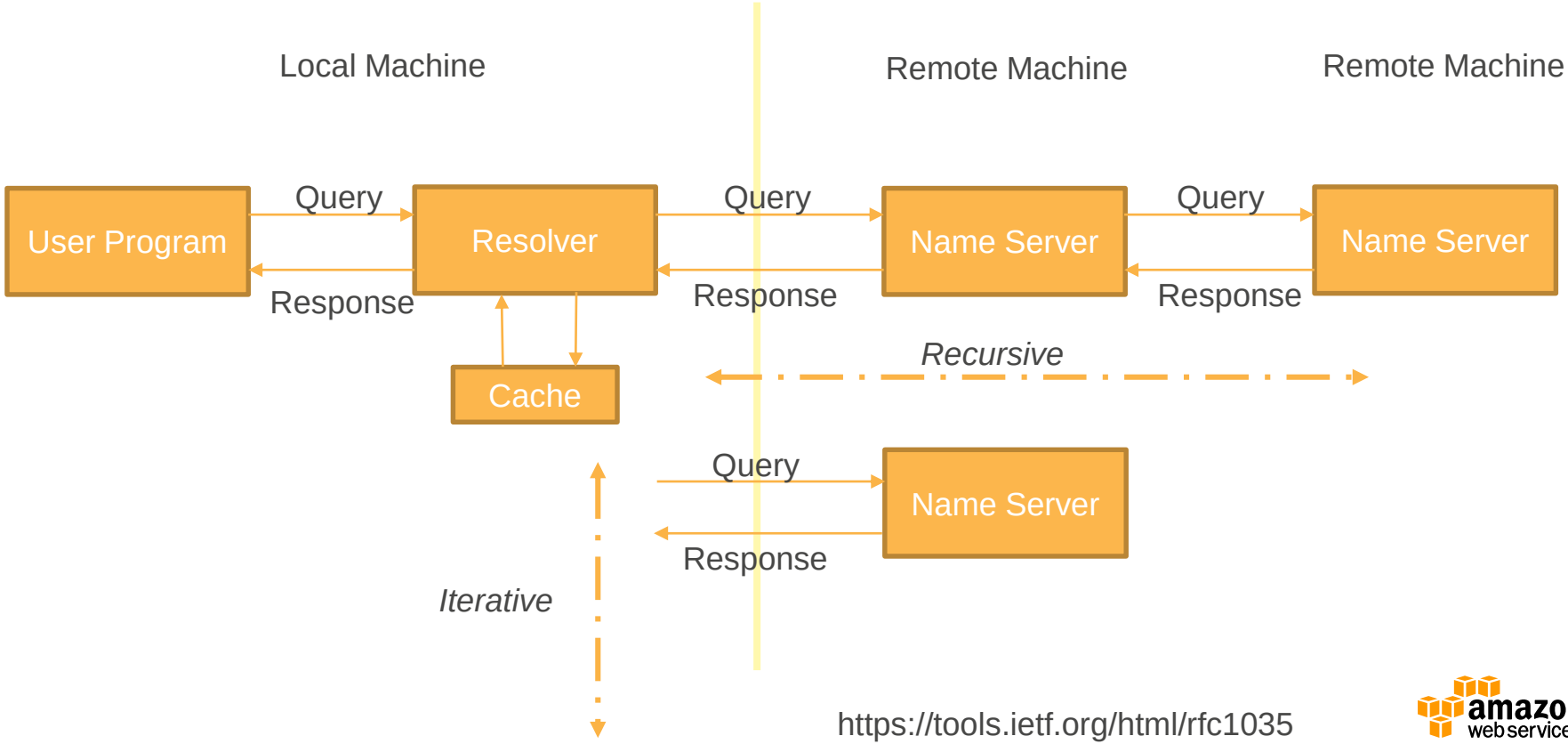
Connect User Requests to Infrastructure

Maps friendly domain names to resources that can process the request

Friendly Name: `aws.amazon.com`

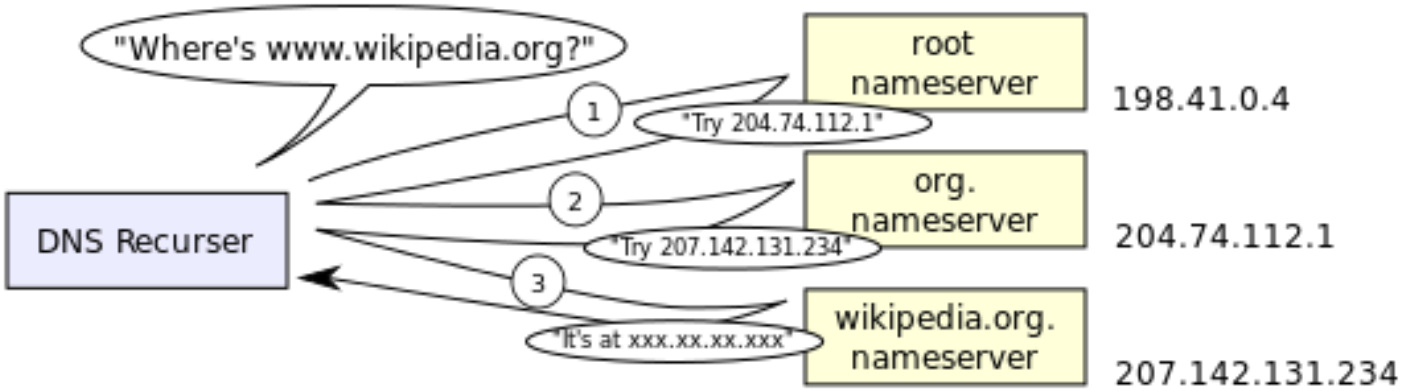
Resource: `54.239.31.69`

Domain Name to IP Address Query



https://tools.ietf.org/html/rfc1035

Example of DNS Query



https://commons.wikimedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg

Demo

- Web Based: http://simpledns.com/lookup-dg.aspx

aws.amazon.com

- Linux: dig <domain> +trace

- Windows: nslookup <domain>

Route 53 Core Capabilities

- Domain Registration & Renewals
- Domain Name Service to map domain names to resource
- Health Check – Route traffic to healthy end points & independently monitor endpoints
- Private DNS – Visible only in attached VPCs
- Global Traffic Management – Route traffic to your globally distributed end points using variety of routing criteria

Route 53 Routing Policy

Routing Policy	Description
Simple Routing	Used when you have a single resource performing a function. For Example, one web server serving content. In Simple Routing, Route 53 simply returns the configured values for matching resource recordset
Weighted Routing	Used when you have multiple resources performing similar function and you want to route traffic to resources in proportions that you specify. For example: Several web servers serving content, A/B testing
Latency Routing	Used when you have deployed your application across multiple regions and want to route customers to resources that offer best possible latency.
Failover Routing	Active-Passive failover support. All traffic is routed to Primary endpoint (known as Active). If primary is down, then all traffic is send to Second endpoint (known as Passive).
Geolocation Routing	Used when you want to route traffic to resources in the same geography as your users. Can be used for compliance requirements. You can support a default record set to handle requests where you don't have resources. Otherwise, Route 53 will return a "No Answer" response

Route 53 and DNS Concepts

Terminology	Description
Generic Top Level Domain (TLD)	Last part of a domain name (.com, .org, .cloud).
Geographic Top Level Domain	Domains associated with geographic areas. (.uk, .fr, .io, .in)
Domain Name System (DNS)	Worldwide network of servers that maintains domain names to IP Addresses
Name Servers (NS)	Servers in DNS that respond to DNS queries
Authoritative Name Server	NS that has definitive information about one part of a domain name

Route 53 and DNS Concepts

Terminology	Description
Hosted Zone – Route 53	A container that has information on how to route traffic for a domain (example.com) and sub domains (www.example.com, retail.example.com)
Resource Record Set	Configuration that maps domain name to resources that can process the request. Several types of resource records are supported
Time To Live (TTL)	Time in Seconds a particular Resource Record Set can be cached
Alias Resource Record Set	Route 53 specific extension to route traffic to AWS resources such ELB, S3, CloudFront and so forth – automatically tracks backend resources. TTL setting is inherited from target service. Cannot change in Route 53

Route 53 Availability and Latency

- Global anycast network designed to answer DNS Queries from optimal location based on network condition – low latency
- Each hosted zone is served by its own set of four virtual name servers - redundancy
- SLA with service credit if uptime percentage drops below the service commitment. When service is not 100% available:
  - 5-30 minutes => 1 day service credit
  - 31 minutes-4hours => 7 days service credit
  - > 4 hours => 30 days service credit
- Changes are propagated to world-wide network of Authoritative DNS Servers within 60 seconds under normal conditions.

Route 53 Record Set

- Record Set is used for specifying DNS configuration details in hosted zone
- Wildcards are supported for domain names
- Every Record Set has a Time To Live (TTL) parameter. This information is used by Resolvers to cache the DNS values
- Route 53 does not have a default TTL for any record type – you must always specify a desired TTL value
- Alias records – that are Route 53 extensions used for pointing to other AWS services inherit TTL values configured in the target service. No option to change the TTL in Route 53.
- Some Record types allow you to specify multiple target values.

Route 53 DNS - Resource Record Types

Record Type	Description	Name	Value
A	IPV4 Address Record. Map domain name to 32 bit IPV4 Address. When queried, returns the IP Address for a given domain name. E.g. Name: example.com Value: 128.0.1.25	Domain Name	IPV4 Address
AAAA	IPV6 Address Record. Map domain name to 128 bit IPV6 Address. When queried, returns the IP Address for a given domain name	Domain Name	IPV6 Address
CNAME	Canonical Alias Record. Alias for a Domain Name (only subdomains or www prefix). Used for mapping one name to another. DNS lookup will continue with the new name. E.g. Name: foo.example.com Value:bar.example.com bar.example.com is an alias for foo.example.com. A client that requests for bar.example.com will get a response foo.example.com.	Domain Name	Alias Name
MX	Mail Exchange Record. Maps a domain name to a list of mail servers that is responsible for accepting email messages on behalf of that domain. Priority of email server is specified using a number. Lowest numbered email server is preferred.	Domain Name	<preference> <email_server_name>

Route 53 DNS - Resource Record Types

Record Type	Description	Name	Value
NS	Naming Server Record. Identifies name servers for a hosted zone. These name servers are responsible for answering queries for the hosted zone. Route 53 assigns four name servers for every hosted zone.	Zone	Name Server Host Name
NAPTR	Naming Authority Pointer Record. Used by Dynamic Delegation Discovery System to convert one value to another or replace one with another. E.g., convert phone numbers to SIP URIs. Allows regular expression based rewriting of domain names which can then be used as URIs	Domain Name	Six configuration values
PTR	Pointer Records. Used for reverse DNS lookup, where for a given IP Address, we need to find the Domain Name.	IP Address backwards	Domain Name
SOA	Start Of (a Zone) Authority Record. Specifies authoritative information about a DNS zone including Primary Name Server, Email of the domain administrator, domain serial number and several timers related to refreshing the zone		Primary Name Server, Email, TTL Values
SPF	Sender Policy Framework. Discontinued. Originally used to verify the identity of the sender of email messages. Replaced by TXT Record		

Route 53 DNS - Resource Record Types

Record Type	Description	Name	Value
SRV	Generalized Service Location Record. Instead of protocol specific records like MX, SRV is a generic record used for newer protocols. SRV record value is made up of four values: Priority, Weight, Port and Host that is providing the service		Four configuration values
TXT	Text Record. Originally for human readable text in a DNS record. Since early 1990s, this record often carries machine readable data such as: opportunistic encryption, SPF, Domain Keys, Domain Keys Identified Mail Records and so forth		Double Quoted String
Alias	Amazon Route 53 Specific extension record. Contains a pointer to a CloudFront Distribution, S3 Bucket, Elastic Beanstalk, ELB/Application Load Balancer, or another Route 53 Resource Record Set in the same hosted zone. Works similar to CNAME allows you to create Alias data. However, differ from CNAME in that it is not visible to resolvers. Resolvers only see the A record and the resulting		Pointer to AWS Resource

Route 53 DNS – Alias Resource Record Types

Alias Record Pointer	Return Value to Query
Alternate domain name for CloudFront Distribution	Route 53 responds as if CloudFront Distribution domain name was requested
Elastic Beanstalk Environment	Route 53 responds to each request with one or more IP addresses for the environment.
ELB load balancer	Route 53 responds to each request with one or more IP addresses for the load balancer.
S3 Bucket configured as Static website	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	Route 53 responds as if the query had asked for the resource record set that is referenced by the pointer

NOTE: You cannot set TTL values for the Alias Pointers. Route 53 uses CloudFront, Elastic BeanStalk, ELB, S3 TTLs or the TTL of Resource Record pointed by Alias

Route 53 automatically handles changes to Alias records. For example, if IP Address of the ELB load balancer changes, Route 53 automatically reflect those changes in answers for the queries

Demo - S3 Static Website

- Access Static Website hosted on S3 using custom domain

Demo - EC2 – Access with Custom Domain

- Launch EC2 Instance
- Install Web Server
- Assign Elastic IP
- Access Website using a custom domain
- Logon to EC2 instance using a well known access point

Demo – RDS Access

- Access Relational Database Service Instance using a custom domain

Demo – Private DNS

- Setup Private Hosted Zone
- Setup RDS access using private application specific access point
- Setup Middleware service access using private application specific end point

Demo – Global Infrastructure - Latency

- Latency Based Routing
- Route Request to instance that gives best performance
- Setup
  - Oregon – 1 web instance
  - Ireland – 1 web instance
  - Frankfurt – 1 Client instance
  - Local PC – 1 Client instance

Demo – Failover Global Infrastructure

Configure Health Checks

- Monitor endpoint
- Aggregate other health checks
- Monitor CloudWatch Metrics

For Private Hosted Zones – Health Checker is outside VPC

- Option 1: Assign a Public IP Address to the instance and monitor with health checker
- Option 2: Indirect monitoring using CloudWatch metrics

Demonstrate how traffic is automatically routed to available instance in a different region

AWS re:Invent Video

DNS Demystified: Amazon Route 53, featuring Warner Bros. (NET202)

Route 53 Traffic Flow

Global Traffic Management Service for your application

Visual Environment to manage

- Globally distributed resources
- Routing Policies
- End Point Health

Traffic Policy – a set of rules that you define to route end users request to your application endpoint

Policy Record – Associates a Traffic Policy to hosted zone

Simplifies creation of resource recordsets, routing policies and other DNS management function

Pricing

$0.50 per Hosted zone / month for first 25 hosted zones. $0.10 for each additional hosted zone per month

- Charged on first day of each month
- To allow testing, hosted zone that is deleted within 12 hours of creation is not charged

Traffic Flow - $50.00 per policy record / month that is associated with DNS name. There is no charge for policy records that are not associated with DNS names

Queries – prorated

- Standard Routing Queries - $0.40 per million queries
- Latency Routing Queries - $0.60 per million queries
- Geolocation Routing Queries - $0.70 per million queries
- Alias Record queries are free

Health Check

- 50 AWS Endpoint health checks free that are linked or within same AWS account
- Basic Health Check (per Health Check / month) - $0.50 on AWS Endpoints and $0.75 on non-AWS Endpoints
- Optional features (per Health Check / month) - $1.00 per optional feature on AWS Endpoints and $2.00 on non-AWS endpoints

Security

Fully integrated with Identity and Access Management (IAM)

Granular access control – limit access to specific

- Hosted Zones
- Health Checks
- Geolocations
- Traffic Policies
- And so forth

Monitoring

Route 53 Health checks

- Sent automatically to CloudWatch at one minute intervals

Metrics

- ChildHealthCheckHealthyCount – Number of healthy checks among all health checks
- ConnectionTime – Average Time in milliseconds to establish connection from health checker to TCP endpoint
- HealthCheckPercentageHealthy – Percentage of health checkers that consider endpoint to be healthy
- HealthCheckStatus – Status of health check endpoint
- SSLHandshakeTime – Average time in milliseconds for Health Checkers to complete SSL handshake
- TimeToFirstByte – Average time in milliseconds for health checkers to receive first byte of the response to a HTTP or HTTPS request

CloudTrail – To capture every request and changes sent to Route 53 API – you must choose US-East (N. Virginia) as region

Private Hosted Zones

- Route traffic for a domain and subdomain within Amazon Virtual Private Cloud (VPCs)
- Only visible within the VPCs associated
- Free to use any domain and subdomain names – no need to register
- VPC must be configured to enable DNS Host Names and DNS Support
- Health checkers are outside of VPC – to check health of an endpoint within VPC,
  - Option 1: Assign a Public IP Address to the instance and monitor with health check
  - Option 2: Indirect monitoring using CloudWatch metrics