Cloud DNS

DNS is a hierarchical distributed database that lets you store IP addresses and other data and look them up by name. Cloud DNS lets you publish your zones and records in DNS without the burden of managing your own DNS servers and software.

Cloud DNS offers both public zones and private managed DNS zones. A public zone is visible to the public internet, while a private zone is visible only from one or more Virtual Private Cloud (VPC) networks that you specify.

Cloud DNS overview

DNS is a hierarchical distributed database that stores IP addresses and other data and allows queries by name.

In other words, DNS is a directory of readable domain names that translate to numeric IP addresses used by computers to communicate with each other. For example, when you type a URL into a browser, DNS converts the URL into an IP address of a web server associated with that name. The DNS directories are stored and distributed around the world on domain name servers that are updated regularly.

The following concepts are useful when working with DNS.

DNS server types

A DNS server stores a database of domain names, and then processes domain names based on DNS queries that come from a client in a network.

Authoritative server

An *authoritative server* is a server that holds the DNS name records, including A, AAAA, and CNAME.

A *non-authoritative server* constructs a cache file based on previous queries for domains. It does not hold original name records.

Recursive resolver

A *recursive resolver* is the server that sends a query to the authoritative or non-authoritative server for resolution. A recursive resolver is so-called because it performs each query for a given name and returns the final result.

This is in contrast to an *iterative resolver*, which only returns a referral to the next DNS servers that might have the answer.

For example, when resolving the name google.com., the recursive resolver must determine who is authoritative for . (the root zone of DNS). Then it asks those name servers who is authoritative for .com. . Finally, it asks those name servers who is authoritative for google.com. , and the rdata for the A record is returned to the client.

Zones

Public zone

A public zone is visible to the internet. You can create DNS records in a public zone to publish your service on the internet. For example, you might create an A record in a public zone called example.com. (note the trailing dot) for your public website www.example.com. .

Private zone

A private zone is any zone that cannot be queried over the public internet.

Records

A record is a mapping between a DNS resource and a domain name. Each individual DNS record has a type (name and number), an expiration time (time to live), and type-specific data.

Some of the commonly used record types are:

- **A:** Address record, which maps host names to their IPv4 address.

- **AAAA:** IPv6 Address record, which maps host names to their IPv6 address.
- **CNAME:** Canonical name record, which specifies alias names.
- **MX:** Mail exchange record, which is used in routing requests to mail servers.
- **NS:** Name server record, which delegates a DNS zone to an authoritative server.
- **PTR:** Pointer record, which defines a name associated with an IP address.
- **SOA:** Start of authority, used to designate the primary name server and administrator responsible for a zone. Each zone hosted on a DNS server must have an SOA (start of authority) record. You can modify the record as needed (for example, you can change the serial number to an arbitrary number to support date-based versioning).

DNSSEC

Cloud DNS supports managed DNSSEC, protecting your domains from spoofing and cache poisoning attacks. When you use a validating resolver like Google Public DNS, DNSSEC provides strong authentication (but not encryption) of domain lookups.

Access control

You can manage the users who are allowed to make changes to your DNS records on the IAM & Admin page in the Google Cloud console. For users to be authorized to make changes, they must have the DNS Administrator role (roles/dns.admin) in the Permissions section of the Google Cloud console. The DNS Reader role (roles/dns.reader) grants read-only access to the Cloud DNS records.

Access control for managed zones

Users with the project Owner role or Editor role (roles/owner or roles/editor) can manage or view the managed zones in the specific project that they are managing.

Users with the DNS Administrator role or DNS Reader role can manage or view the managed zones across all the projects that they have access to.

Project Owners, Editors, DNS Administrators, and DNS Readers can view the list of private zones applied to any VPC network in the current project.