What Is a DNS Record, and How to Set it?

No comments

Domain Name Systems (DNS) serve as the phonebook for the Internet. Information is accessed online through domain names such as nytimes.com and espn.com. Web browsers communicate with each other through IP addresses. DNS translates domain names into IP addresses, so browsers can access Internet resources. When the DNS server returns an IP address, the browser connects to the webpage that appears on your screen. Users are not aware of the background tasks involved in making the system work. If the DNS server is unavailable, the browser cannot acquire the IP address of the website, so it returns an error.

What Is DNS?

A domain name system (DNS) enables humans to access information online. Web browsers use Internet Protocol (IP) addresses to interact with each other. Domain names are translated into IP addresses by DNS so that Internet resources can be accessed by browsers. An IP address is assigned to each device connected to the Internet so that other computers can locate it. DNS servers eliminate the need for humans to memorize IP addresses like 192.168.1.1 (for

IPv4), or more complex newer alphanumeric IP addresses like 2400:cb00:2048:1::c629:d7a2 (for IPv6)).

What Is a DNS Record?

There are DNS records (also known as zone files) that reside on authoritative DNS servers and provide information about a domain, including what IP address is associated with the domain and how to handle requests for it. The DNS syntax is used to write a series of text files that make up DNS records. DNS syntax is simply a string of characters that tells the DNS server what to do.

'TTL', which stands for time-to-live, indicates how frequently a DNS server will refresh a record. DNS records can be compared to business listings on Yelp. They provide information such as the business's address, hours, services offered, etc. For a user to be able to access a domain's website using a domain name, there are several essential DNS records, as well as several optional records that serve additional purposes.

How Does DNS Work?

An IP address is assigned to each device on the Internet, and that address is necessary to find the appropriate Internet device - as a street address is necessary to find a particular home. In DNS resolution, a hostname (such as www.example.com) is converted into an IP address (such as 192.168.1.1). It is necessary to translate what a user types into their web browser (example.com) into the machine-friendly address needed to locate the example.com website.

The process behind DNS resolution can be understood best if you understand the different hardware components a query must pass through. Web browsers perform DNS lookups "behind the scenes" and do not require any interaction other than the initial request from the user.

The Four DNS Servers involved in loading a Website

1. DNS Recursor

DNS recursors are analogous to librarians responsible for finding specific books in libraries. they receive queries from clients via web browsers. In most cases, the recursor is responsible for making additional requests to fulfill the client's DNS request.

2. Root Nameserver

This server serves as the first step in translating (resolving) human readable host names into IP addresses; it is like an index in a library pointing to books in different racks.

3. TLD Nameserver

Nameservers are the next step in the search for an IP address, and they host the last portion of a hostname (For example, in example.com, the TLD server is "com ").

4. Authoritative Nameserver

A final nameserver can be thought of as a dictionary on a shelf full of books, where a particular name can be translated into its definition. It is the last point on the nameserver query. This is where the authoritative nameserver (the librarian) returns the IP address for the requested hostname back to the DNS Recursor (the query maker).

Image not found or type unknown

What Is a DNS Record, and How to Set it?

Authoritative DNS Servers vs. Recursive DNS Resolvers: What's the Difference?

As well as serving as integral parts of the DNS infrastructure, both concepts refer to servers (groups of servers) that perform different roles and reside in different locations within the DNS query pipeline. The recursive resolver is at the beginning of a DNS query, whereas the authoritative nameserver is at the end.

Recursive DNS Resolver

In response to recursive requests from clients, resolvers track down DNS records. They do this by making a series of requests until the authoritative DNS nameserver for the requested record is reached (or times out or returns an error if it does not find a record)).

Fortunately, recursive DNS resolvers don't always need to make multiple requests to track down the records needed to respond to a client. Caching is a method of data persistence that short-circuits the necessary requests by serving the requested resource record sooner in the DNS lookup.

Authoritative DNS Server

DNS authoritative servers are servers that actually store, and are responsible for, DNS resource records. This is the server at the bottom of a DNS lookup chain that responds with the requested resource record, which ultimately allows a web browser to reach the IP address for a website or other web resource. Authoritative nameservers can satisfy queries from their own data without querying another source since they are the definitive source of truth for certain DNS records.

Setting up a DNS Entry for the Web Server

A website's accessibility is obviously one of the most important things about running it. Part of this process involves setting up CNAME (Canonical Name) records on the DNS server where IIS (Internet Information Services) is configured. By following this step, external computers can connect to your Web server using the “www” hostname. Follow these steps to create a new DNS entry:

1. Open the DNS snap-in by clicking Start -> Administrative Tools -> DNS.

2. Once DNS has been opened, expand "Hostname" (where "Hostname" means the hostname of your DNS server).

3. Select the Forward Lookup Zones option.

4. In the Forward Lookup Zones section, right-click the zone you wish to alias (for example, domain_name.com) and click New Alias (CNAME).

5. Type “www.” in the Alias name box.

6. Finally, in the Fully qualified name for the target host box, enter the name of the DNS server where IIS is installed (for example, dns.domain_name.com).

7. To complete your changes, click OK.

Secure Recursive DNS

Recursive lookups occur when a DNS server is queried for a domain it is not authoritative. An example would be querying your nameserver for the domain yahoo.com. It is based on this principle that DNS recursion, also known as an open DNS server, occurs when your DNS server is available to the public for DNS lookups. If you have an open DNS server, there is a higher chance that your server will get abused by spammers. Moreover, open DNS recursion consumes a lot of resources.

To lighten the load on your server and reduce potential risk, you can restrict recursive and caching lookups to only the IP blocks listed in the configuration. Using this method, hackers and malicious actors can reduce the risk associated with DNS exploitation. Firstly, follow the instructions specific to your server's OS. we've included both Linux and Windows instructions.

Linux Servers

The file /etc/named.conf needs to be modified on Linux servers running Bind to ensure recursion security. Note: If you make any changes, please back up the file to make sure nothing is lost. In the example below, the first line of the "allow-recursion" command is set for IP address 127.0.0.1.

Assuming the server has a nameserver 127.0.0.1, this allows the local Linux machine to query this specific IP address (127.0.0.1). Additionally, you can edit these lines to include only the subnets you require or prefer if you want your DNS to be even more secure.

```
options {
 recursion yes;
 allow-recursion { 127.0.0.1/32; };
 allow-query-cache { 127.0.0.1/32; };
}
```

Whenever you make changes to Bind, restart it by running the following command:

service named restart

or

/etc/init.d/named restart

Conclusion

The Internet is a world of numbers, and all computers use them to find and communicate with one another, whether they are smartphones or laptops or servers that serve content to gigantic retail websites. IP addresses are these numbers. You don't need to remember and enter a long number when you open a web browser and visit a website. By entering a domain name such as example.com, you will still end up in the right place.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.

Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP NEWSLETTER RSS FEED