«Una introducción a la terminología, componentes y conceptos de DNS» por Justin Ellingwood

---

«Una introducción a la terminología, componentes y conceptos de DNS» por Justin Ellingwood.

Introducción

El DNS, o el Sistema de Nombres de Dominio, es a menudo una parte muy difícil de aprender sobre el cómo configurar sitios web y servidores. Comprender cómo funciona el DNS le ayudará a diagnosticar problemas con la configuración del acceso a sus sitios web y le permitirá ampliar su comprensión de lo que está sucediendo entre bambalinas.

En esta guía, analizaremos algunos conceptos de DNS fundamentales que lo ayudarán a comenzar a ejecutar su configuración de DNS. Después de abordar esta guía, deberá estar listo para configurar su nombre de dominio con DigitalOcean o configurar su propio servidor DNS.

Antes de pasar a configurar sus propios servidores para resolver su dominio o configurar nuestros dominios en el panel de control, repasemos algunos conceptos básicos sobre cómo funciona todo esto.

Terminología de dominio

Debemos comenzar por definir nuestros términos. Si bien algunos de estos temas son familiares en otros contextos, hay muchos términos que se usan cuando se habla de nombres de dominio y DNS que no se usan con demasiada frecuencia en otras áreas de la informática.

Comencemos de manera sencilla:

Sistema de Nombres de Dominio

El Sistema de Nombres de Dominio, más comúnmente conocido como "DNS" es el que viene incorporado en el sistema de redes el cual nos permite resolver nombres amigables para el hombre en direcciones únicas.

Nombre de dominio

Un nombre de dominio es el nombre amigable para el ser humano que estamos acostumbrados a asociar con un recurso de Internet. Por ejemplo, "google.com" es un nombre de dominio. Algunas personas dirán que la parte "google" es el dominio, pero generalmente podemos referirnos a la forma combinada como el nombre de dominio.

La URL "google.com" está asociada con los servidores propiedad de Google Inc. El sistema de nombres de dominio nos permite acceder a los servidores de Google cuando escribimos "google.com" en nuestros navegadores.

Dirección IP

Una dirección IP es lo que llamamos una ubicación direccional de la red. Cada dirección IP debe ser única dentro de su red. Cuando hablamos de sitios web, esta red es todo el Internet.

IPv4, la forma más común de direcciones, se escriben como cuatro conjuntos de números, cada uno de los cuales tiene hasta tres dígitos y cada conjunto está separado por un punto. Por ejemplo, "111.222.111.222" podría ser una dirección IP válida de IPv4. Con DNS, asignamos un nombre a esa dirección para que no tenga que recordar un conjunto complicado de números para cada lugar que desee visitar en una red.

Dominio de primer nivel

Un dominio de nivel superior, o TLD, es la parte más general del dominio. El dominio de nivel superior es la parte más alejada a la derecha (separado por un punto). Los dominios comunes de nivel superior son "com", "net", "org", "gov", "edu" e "io".

Los dominios de nivel superior están en la parte superior de la jerarquía en términos de nombres de dominio. La ICANN (Corporación de Internet para la Asignación de Nombres y Números) otorga a ciertas partes el control de la administración sobre los dominios de nivel superior. Estas partes pueden distribuir nombres de dominio bajo el TLD, generalmente a través de un registrador de dominio.

Anfitriones

Dentro de un dominio, el propietario del dominio puede definir anfitriones individuales, que se refieren a computadoras o servicios separados accesibles a través de un dominio. Por ejemplo, la

mayoría de los propietarios de dominios hacen que sus servidores web sean accesibles a través del dominio simple ("ejemplo.com") y también a través de la definición de anfitrión " www" ("www.ejemplo.com").

Puede tener otras definiciones de anfitrión bajo el dominio general. Podría tener acceso a la API a través de un anfitrión "api" (api.ejemplo.com) o podría tener acceso FTP definiendo un anfitrión llamado "ftp" o "archivos" (ftp.ejemplo.com o archivos.ejemplo.com). Los nombres de anfitriones pueden ser arbitrarios siempre y cuando sean únicos para el dominio.

SubDominio

Un tema relacionado con los anfitriones son los subdominios.

DNS trabaja en una jerarquía. Los TLD pueden tener muchos dominios debajo de ellos. Por ejemplo, el TLD "com" tiene tanto "google.com" como "ubuntu.com" debajo de él. Un "subdominio" se refiere a cualquier dominio que sea parte de un dominio más grande. En este caso, se puede decir que "ubuntu.com" es un subdominio de "com". Por lo general, esto se denomina simplemente dominio o la porción "ubuntu" se denomina SLD, lo que significa un dominio de segundo nivel.

Del mismo modo, cada dominio puede controlar "subdominios" que se encuentran debajo de él. Generalmente esto suele ser lo que entendemos por subdominios. Por ejemplo, podría tener un subdominio para el departamento de historia de su escuela en "www.historia.escuela.edu". La parte de "historia" es un subdominio.

La diferencia entre un nombre de anfitrión y un subdominio es que un anfitrión define una computadora o recurso, mientras que un subdominio extiende el dominio principal. Es un método de subdividir el propio dominio.

Ya sea al hablar de subdominios o anfitriones, puede comenzar a ver que las partes más a la izquierda de un dominio son las más específicas. Así es como funciona el DNS: de más a menos específico a medida que lee de izquierda a derecha.

Nombre de dominio completamente calificado

Un nombre de dominio completamente calificado, a menudo llamado FQDN, es lo que llamamos un nombre de dominio absoluto. Los dominios en el sistema DNS se pueden dar unos en relación con otros, y como tales, pueden ser algo ambiguos. Un FQDN es un nombre absoluto que especifica su ubicación en relación con la raíz absoluta del sistema de nombres de dominio.

Esto significa que especifica cada dominio principal, incluido el TLD. Un FQDN adecuado termina con un punto, que indica la raíz de la jerarquía de DNS. Un ejemplo de un FQDN es "mail.google.com". A veces, el software que requiere FQDN no requiere el punto final, pero se

requiere que el punto final se ajuste a los estándares de la ICANN.

Servidor de Nombres

Un servidor de nombres es una computadora designada para traducir nombres de dominio a direcciones IP. Estos servidores hacen la mayor parte del trabajo en el sistema DNS. Dado que el número total de traducciones de dominio es demasiado alto para cualquier servidor, cada servidor puede redirigir la solicitud a otros servidores de nombres o delegar la responsabilidad de un subconjunto de subdominios de los que son responsables.

Los servidores de nombres pueden ser "autorizados", lo que significa que dan respuestas a las consultas sobre dominios bajo su control. De lo contrario, pueden apuntar a otros servidores o servir copias en caché de los datos de otros servidores de nombres.

Archivo de zona

Un archivo de zona es un archivo de texto simple que contiene las asignaciones entre nombres de dominio y direcciones IP. Así es como el sistema DNS finalmente descubre con qué dirección IP se debe contactar cuando un usuario solicita un determinado nombre de dominio.

Los archivos de zona residen en servidores de nombres y generalmente definen los recursos disponibles bajo un dominio específico, o el lugar al que uno puede ir para obtener esa información.

Registros

Dentro de un archivo de zona, los registros se mantienen. En su forma más simple, un registro es básicamente una asignación única entre un recurso y un nombre. Estos pueden asignar un nombre de dominio a una dirección IP, definir los servidores de nombres para el dominio, definir los servidores de correo para el dominio, etc.

Cómo funciona el DNS

Ahora que está familiarizado con algunos de los términos relacionados con DNS, ¿cómo funciona realmente el sistema?

El sistema es muy simple en una visión general de alto nivel, pero es muy complejo al mirar los detalles. Sin embargo, en general, es una infraestructura muy confiable que ha sido esencial para la adopción de Internet tal como lo conocemos hoy.

Servidores Raíz

Como dijimos anteriormente, el DNS es, en esencia, un sistema jerárquico. En la parte superior de este sistema se encuentran los "servidores raíz". Estos servidores están controlados por varias organizaciones y están delegados por la ICANN (Corporación de Internet para la Asignación de Nombres y Números).

Actualmente hay 13 servidores raíz en operación. Sin embargo, como hay una cantidad increíble de nombres para resolver cada minuto, cada uno de estos servidores está reflejado. Lo interesante de esta configuración es que cada una de las réplicas de un solo servidor raíz comparte la misma dirección IP. Cuando se realizan solicitudes para un determinado servidor raíz, la solicitud se encaminará al servidor espejo más cercano de ese servidor raíz.

¿Qué hacen estos servidores raíz? Los servidores raíz manejan las solicitudes de información sobre dominios de nivel superior. Entonces, si se recibe una solicitud para algo que un servidor de nombres de nivel inferior no puede resolver, se realiza una consulta al servidor raíz para el dominio.

Los servidores raíz no sabrán realmente dónde está alojado el dominio. Sin embargo, podrán dirigir al solicitante a los servidores de nombres que manejan el dominio de nivel superior solicitado específicamente.

Entonces, si se realiza una solicitud de "www.wikipedia.org" al servidor raíz, el servidor raíz no encontrará el resultado en sus registros. Verificará sus archivos de zona para una lista que coincida con "www.wikipedia.org". No encontrará uno.

En su lugar, encontrará un registro para el TLD "org" y le dará a la entidad solicitante la dirección del servidor de nombres responsable de las direcciones "org".

Servidores de TLD

El solicitante luego envía una nueva solicitud a la dirección IP (que le proporciona el servidor raíz) que es responsable del dominio de nivel superior de la solicitud.

Entonces, para continuar con nuestro ejemplo, enviaría una solicitud al servidor de nombres responsable de conocer los dominios "org" para ver si sabe dónde se encuentra "www.wikipedia.org".

Una vez más, el solicitante buscará "www.wikipedia.org" en sus archivos de zona. No encontrará este registro en sus archivos.

Sin embargo, encontrará un registro con la dirección IP del servidor de nombres responsable de "wikipedia.org". Esto se está acercando mucho más a la respuesta que queremos.

Servidores de nombres a nivel de dominio

En este punto, el solicitante tiene la dirección IP del servidor de nombres que es responsable de conocer la dirección IP real del recurso. Envía una nueva solicitud al servidor de nombres preguntando, una vez más, si puede resolver "www.wikipedia.org".

El servidor de nombres comprueba sus archivos de zona y encuentra que tiene un archivo de zona asociado con "wikipedia.org". Dentro de este archivo, hay un registro para el host "www". Este registro indica la dirección IP donde se encuentra este host. El servidor de nombres devuelve la respuesta final al solicitante.

¿Qué es un Servidor de Resolución de Nombres?

En el escenario anterior, nos referimos a un "solicitante". ¿Cuál es el solicitante en esta situación?

En casi todos los casos, el solicitante será lo que llamamos un "Servidor de Resolución de Nombres". Un Servidor de Resolución de Nombres está configurado para hacer preguntas a otros servidores. Básicamente, es un intermediario para un usuario que almacena en caché los resultados de las consultas anteriores para mejorar la velocidad y conoce las direcciones de los servidores raíz para poder "resolver" las solicitudes de cosas que aún no conoce.

Básicamente, un usuario generalmente tendrá unos pocos Servidores de Resolución de Nombres configurados en su sistema informático. Los Servidores de Resolución de Nombres suelen ser proporcionados por un ISP u otras organizaciones. Por ejemplo, Google proporciona servidores de resolución de DNS(en idioma inglés) que usted puede usar para consultar. Estos pueden ser configurados en su computadora automáticamente o manualmente.

Cuando escribe una URL en la barra de direcciones de su navegador, su computadora primero ve si puede encontrar localmente en dónde se encuentra el recurso. Comprueba el archivo llamado "hosts" en la computadora y en algunas otras ubicaciones. Luego envía la solicitud al servidor de nombres de resolución y espera para recibir la dirección IP del recurso.

El Servidor de Resolución de Nombres comprueba su caché para la respuesta. Si no lo encuentra, sigue los pasos descritos anteriormente.

La resolución de los servidores de nombres básicamente comprime el proceso de solicitud para el usuario final. Los clientes simplemente deben saber preguntar a los Servidores de Resolución de Nombres dónde se encuentra un recurso y tener la confianza de que ellos investigarán y devolverán la respuesta final.

Archivos de zona

Mencionamos en el proceso anterior las ideas de "archivos de zona" y "registros".

Los archivos de zona son la forma en que los servidores de nombres almacenan información sobre los dominios que conocen. Cada dominio que un servidor de nombres conoce se almacena en un archivo de zona. La mayoría de las solicitudes que llegan al servidor de nombres promedio no son algo para lo que el servidor tendrá archivos de zona.

Si está configurado para manejar consultas recursivas, como un Servidor de Resolución de Nombres, encontrará la respuesta y la devolverá. De lo contrario, le dirá a la parte solicitante dónde buscar a continuación.

Cuantos más archivos de zona tenga un Servidor de Nombres, más solicitudes podrá responder con autoridad.

Un archivo de zona describe una "zona" de DNS, que es básicamente un subconjunto de todo el sistema de nombres de DNS. Generalmente se usa para configurar un solo dominio. Puede contener una serie de registros que definen dónde están los recursos para el dominio en cuestión.

La variable $ORIGIN de la zona es un parámetro igual al nivel más alto de autoridad de la zona por defecto.

Por lo tanto, si se usa un archivo de zona para configurar el dominio "ejemplo.com.", el $ORIGIN se establecería en "ejemplo.com." .

Esto se configura en la parte superior del archivo de zona o se puede definir en el archivo de configuración del servidor DNS que hace referencia al archivo de zona. De cualquier manera, este parámetro describe para qué estará autorizada la zona.

De manera similar, $TTL configura el "tiempo de vida" de la información que proporciona. Es básicamente un temporizador. Un servidor de nombres de almacenamiento en caché puede usar los resultados consultados previamente para responder preguntas hasta que se agote el valor TTL.

Tipos de registro

Dentro del archivo de zona, podemos tener muchos tipos de registros diferentes. Vamos a repasar algunos de los más comunes (algunos de tipo obligatorio) aquí.

Registros SOA

El registro de Autoridad de la Zona, o SOA, es un registro obligatorio en todos los archivos de zona. Debe ser el primer registro real en un archivo (aunque las especificaciones de $ORIGIN o

$TTL pueden aparecer arriba). También es uno de los más complejos de entender.

El registro de inicio de autoridad se ve como algo así:

```
dominio.com.
  IN SOA ns1.dominio.com. admin.dominio.com. (
                 12083   ; número de serial

                          3h      ;
 intervalo de refrescamiento

                          30m     ;
 intervalo de reintento

                          3w      ;
 tiempo de expiración
                                          1h      ; TTL negativo )
```

Vamos a explicar para qué es cada parte:

- **dominio.com .**: Esta es la raíz de la zona. Esto especifica que el archivo de zona es para el dominio dominio.com.. A menudo, usted verá que esto se reemplaza con @, que es solo un marcador de posición que sustituye el contenido de la variable $ORIGIN que aprendimos anteriormente.
- **IN SOA**: La parte "IN" significa Internet (y estará presente en muchos registros). La SOA es el indicador de que este es un registro de inicio de autoridad.
- **ns1.dominio.com .**: Esto define el servidor de nombres maestro primario para este dominio. Los servidores de nombres pueden ser maestros o esclavos, y si el DNS dinámico está configurado, un servidor debe ser un "maestro primario", el cual entonces se incluye aquí. Si no ha configurado el DNS dinámico, este es solo uno de sus servidores de nombres maestros.
- **admin.dominio.com.**: Esta es la dirección de correo electrónico del administrador de esta zona. La "@" se reemplaza con un punto en la dirección de correo electrónico. Si la parte del nombre de la dirección de correo electrónico normalmente tiene un punto, se reemplaza con un "\" en esta parte (su.nombre@dominio.com se convierte en su\nombre.dominio.com).
- **12083**: Este es el número de serie del archivo de zona. Cada vez que edite un archivo de zona, debe incrementar este número para que el archivo de zona se propague correctamente. Los servidores esclavos verificarán si el número de serie del servidor maestro para una zona es más grande que el que tienen en su sistema. Si es así, solicita

el nuevo archivo de zona, si no, continúa sirviendo el archivo original.
- **3h**: Este es el intervalo de actualización para la zona. Esta es la cantidad de tiempo que el esclavo esperará antes de sondear el maestro para los cambios de archivo de zona.
- **30m**: Este es el intervalo de reintento para esta zona. Si el esclavo no puede conectarse al maestro cuando finaliza el período de actualización, esperará esta cantidad de tiempo y volverá a intentar sondear el maestro.
- **3w**: Este es el periodo de expiración. Si un servidor de nombres esclavo no ha podido ponerse en contacto con el maestro durante este período de tiempo, ya no devolverá las respuestas como una fuente autorizada para esta zona.
- **1h**: Esta es la cantidad de tiempo que el servidor de nombres almacenará en la memoria caché un error de nombre si no puede encontrar el nombre solicitado en este archivo.

Registros A y AAAA

Ambos registros asignan un anfitrión a una dirección IP. El registro "A" se usa para asignar un anfitrión a una dirección IP IPv4, mientras que los registros "AAAA" se usan para asignar un anfitrión a una dirección IPv6.

El formato general de estos registros es el siguiente:

```
anfitrión IN A dirección_IPv4 anfitrión IN AAAA dirección_IPv6
```

Por lo tanto, dado que nuestro registro SOA llamó a un servidor maestro primario en "ns1.dominio.com", tendríamos que mapear esta dirección a una dirección IP ya que "ns1.dominio.com" está dentro de la zona "dominio.com" que precisamente este archivo está definiendo.

El registro podría verse algo parecido a esto:

```
ns1     IN  A       111.222.111.222
```

Tenga en cuenta que no tenemos que dar el nombre completo. Solo podemos dar el host, sin el FQDN y el servidor DNS completará el resto con el valor $ORIGIN. Sin embargo, podríamos usar el FQDN completo con la misma facilidad si queremos ser semánticos:

```
ns1.dominio.com.     IN  A       111.222.111.222
```

En la mayoría de los casos, aquí es donde definirá su servidor web como "www":

```
www     IN  A       222.222.222.222
```

También debemos decir dónde se resuelve el dominio base. Podemos hacer esto así:

```
domain.com.     IN  A       222.222.222.222
```

Podríamos haber usado la "@" para referirnos al dominio base en su lugar:

```
@       IN  A       222.222.222.222
```

También tenemos la opción de resolver cualquier cosa que, bajo este dominio, no esté definida explícitamente para este servidor. Podemos hacer esto con el comodín "*":

```
*       IN  A       222.222.222.222
```

Todos estos funcionan igual de bien con los registros AAAA para direcciones IPv6.

Registros CNAME

Los registros CNAME definen un alias para el nombre canónico de su servidor (uno definido por un registro A o AAAA).

Por ejemplo, podríamos tener un registro de nombre A que defina el anfitrión "servidor1" y luego usar "www" como un alias para este anfitrión:

```
servidor1   IN  A       111.111.111.111 www         IN  CNAME   servidor1
```

Tenga en cuenta que estos alias vienen con algunas pérdidas de rendimiento porque requieren una consulta adicional al servidor. La mayoría de las veces, se puede lograr el mismo resultado utilizando registros A o AAAA adicionales.

Un caso cuando se recomienda un CNAME es proporcionar un alias para un recurso fuera de la zona actual.

Registros MX

Los registros MX se utilizan para definir los intercambios de correo que se utilizan para el dominio. Esto ayuda a que los mensajes de correo electrónico lleguen a su servidor de correo correctamente.

A diferencia de muchos otros tipos de registros, los registros de correo generalmente no asignan un anfitrión a algo, porque se aplican a toda la zona. Como tal, usualmente se ven así:

```
        IN  MX  10   mail.dominio.com.
```

Tenga en cuenta que no hay un nombre de anfitrión al principio.

También tenga en cuenta que hay un número adicional allí. Este es el número de preferencia que ayuda a las computadoras a decidir a qué servidor enviar correos si hay varios servidores de correo definidos. Los números más bajos tienen una prioridad más alta.

El registro MX generalmente debe apuntar a un anfitrión definido por un registro A o AAAA, y no uno definido por un CNAME.

Entonces, digamos que tenemos dos servidores de correo. Tendría que haber registros que se parezcan a esto:

```
        IN  MX  10  mail1.dominio.com.         IN  MX  50  mail2.dominio.
com. mail1   IN  A       111.111.111.111 mail2   IN  A       222.222.222.
222
```

En este ejemplo, el anfitrión "mail1" es el servidor de intercambio de correo electrónico preferido.

También podríamos escribirlo así:

```
        IN  MX  10  mail1         IN  MX  50  mail2 mail1   IN  A       1
11.111.111.111 mail2   IN  A       222.222.222.222
```

Registros de NS

Este tipo de registro define los servidores de nombres que se utilizan para esta zona.

Quizás se esté preguntando, "si el archivo de zona reside en el servidor de nombres, ¿por qué necesita hacer referencia a sí mismo?". Parte de lo que hace que DNS sea tan exitoso son sus múltiples niveles de almacenamiento en caché. Una razón para definir los servidores de nombres dentro del archivo de zona es que el archivo de zona puede realmente ser servido desde una copia en caché en otro servidor de nombres. Hay otras razones para necesitar que los servidores de nombres se definan en el servidor de nombres en sí, pero no lo veremos aquí.

Al igual que los registros MX, estos son parámetros de toda la zona, por lo que tampoco toman anfitrión. En general, se ven así:

```
        IN  NS     ns1.dominio.com.         IN  NS     ns2.dominio.com.
```

Usted debe tener al menos dos servidores de nombres definidos en cada archivo de zona para funcionar correctamente en caso de que haya un problema con un servidor. La mayoría del software del servidor DNS considera que un archivo de zona no es válido si solo hay un único servidor de nombres.

Como siempre, incluya la asignación para los anfitrión con registros A o AAAA:

```
        IN  NS     ns1.dominio.com.         IN  NS     ns2.dominio.com. n
s1     IN  A      111.222.111.111 ns2     IN  A      123.211.111.233
```

Hay muchos otros tipos de registros que puede usar, pero estos son probablemente los tipos más comunes con los que se encontrará.

Registros PTR

Los registros PTR que se utilizan definen un nombre asociado con una dirección IP. Los registros PTR son el inverso de un registro A o AAAA. Los registros PTR son únicos, ya que comienzan en la raíz .arpa y se delegan a los propietarios de las direcciones IP. Los Registros Regionales de Internet (RIR) administran la delegación de direcciones IP a los proveedores de servicios y organización. Los Registros Regionales de Internet incluyen APNIC, ARIN, RIPE NCC, LACNIC y AFRINIC.

Este es un ejemplo de un registro PTR para 111.222.333.444 que se vería así:

```
444.333.222.111.in-addr.arpa.   33692   IN  PTR anfitrión.ejemplo.com.
```

Este ejemplo de un registro PTR para una dirección IPv6 muestra el *formato de cuarteto* del reverso del servidor DNS IPv6 de Google: 2001:4860:4860::8888:

```
8.8.8.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.8.4.0.6.8.4.1.0.0.2.ip6.arpa.
 86400IN PTR google-public-dns-a.google.com.
```

La herramienta de línea de comandos **dig** con el indicador -x se puede usar para buscar el nombre DNS inverso de una dirección IP.

Aquí hay un ejemplo de un comando de **dig**. El +SHORT se adjunta para reducir la salida al nombre DNS inverso.

```
$ dig -x 8.8.4.4 +short
```

La salida para el comando **dig** anterior será el nombre de dominio en el registro PTR para la dirección IP:

```
google-public-dns-b.google.com.
```

Los servidores en Internet utilizan los registros PTR para colocar nombres de dominio en las entradas del registro, tomar decisiones sobre el manejo del *correo basura* notificado y mostrar detalles fáciles de leer sobre otros dispositivos.

Los servidores de correo electrónico más utilizados buscarán el registro PTR de una dirección IP de la que recibe correo electrónico. Si la dirección IP de origen no tiene un registro PTR asociado, los correos electrónicos que se envíen pueden tratarse como correo no deseado y rechazarse. No es importante que el FQDN en el PTR coincida con el nombre de dominio del correo electrónico que se envía. Lo que es importante es que haya un registro PTR válido con un registro A correspondiente y coincidente de retorno.

Normalmente, los enrutadores de red en Internet reciben registros PTR que se corresponden con su ubicación física. Por ejemplo, puede ver referencias a 'NYC' o 'CHI' para un enrutador en la ciudad de Nueva York o Chicago. Esto es útil cuando se ejecuta un traceroute o MTR(en idioma inglés) y se revisa la ruta que está tomando el tráfico de Internet.

La mayoría de los proveedores que ofrecen servidores dedicados o servicios de VPS brindarán a los clientes la capacidad de establecer un registro PTR para su dirección IP. **DigitalOcean asignará automáticamente el registro PTR de cualquier Droplet cuando la Droplet tenga un nombre de dominio.** El nombre de Droplet se asigna durante la creación y se puede editar más tarde utilizando la página de configuración del panel de control de Droplet.

> Nota: Es importante que el FQDN en el registro PTR tenga un registro A ccorrespondiente y coincidente de retorno. Ejemplo: 111.222.333.444 tiene un PTR de servidor.ejemplo.com y servidor.ejemplo.com es un registro A que apunta a 111.222.333.444.

Registros CAA

Los registros CAA se utilizan para especificar qué Autoridades de certificado (CA) pueden emitir certificados SSL / TLS para su dominio. A partir del 8 de septiembre de 2017, todas las CA deben verificar estos registros antes de emitir un certificado. Si no hay registro presente, cualquier CA puede emitir un certificado. De lo contrario, solo las CA especificadas pueden emitir certificados. Los registros de CAA se pueden aplicar a anfitriones únicos o dominios completos.

Un ejemplo de registro CAA sigue:

```
ejemplo.com.    IN  CAA 0 issue "letsencrypt.org"
```

El anfitrión, IN y el tipo de registro (CAA) son campos de DNS comunes. La información específica de CAA anterior es la porción de 0 issue "letsencrypt.org". Se compone de tres partes: indicadores (0), etiquetas (issue) y valores ("letsencrypt.org").

- Las **banderas** *("**Flags**")* son números enteros que indican cómo una CA debe manejar las etiquetas que no entiende. Si la bandera es 0, el registro será ignorado. Si es 1, la CA debe negarse a emitir el certificado.
- Las **etiquetas** ("***Tags***") son cadenas que denotan el propósito de un registro CAA. Actualmente, se puede emitir para autorizar a una CA a crear certificados para un nombre

de anfitrión específico, issuewild para autorizar certificados con comodines o iodef para definir una URL donde las CA pueden informar violaciones de políticas.
- Los **valores** *("**Values**")* son una cadena asociada con la etiqueta del registro. Para issue y issuewild, este será típicamente el dominio de la CA a la que usted esté otorgando el permiso. Para iodef, esta puede ser la URL de un formulario de contacto o un enlace mailto:link para recibir comentarios por correo electrónico.

Puede usar **dig** para buscar registros CAA usando las siguientes opciones:

```
$ dig ejemplo.com type257
```

Para una información detallada acerca de los registros CAA, usted puede consultar la norma RFC 6844,(en idioma inglés) or nuestro tutorial acerca sobre «Cómo crea y administrar registros CAA por medio de los DNS de DigitalOcean»(en idioma inglés).

Conclusión

Ahora deberías tener un buen conocimiento de cómo funciona el DNS. Si bien la idea general es relativamente fácil de entender una vez que está familiarizado con la estrategia, esto sigue siendo algo que puede ser difícil de poner en práctica para los administradores inexpertos.

Para una visión general eche un vistazo a «Cómo configurar dominios web con el Panel de Control en DigitalOcean»(en idioma inglés).