

Guías y Manuales

Que es una zona DNS y respectivos registros?

Un 'archivo de zona' o zona dns es un archivo que contiene los datos para poder resolver las peticiones de nombres asociadas al dominio en direcciones IP.

FORMATO GENERAL DE UN ARCHIVO DNS Y TIPOS DE REGISTROS:

REGISTROS SOA

El primer registro de cualquier archivo de base de datos es el registro SOA. Este registro se forma con una serie de parámetros a tener en cuenta.

Host origen: El host en el que se mantiene el archivo.

Correo electrónico de contacto: La dirección de correo electrónico de Internet de la persona responsable del archivo de base de datos de este dominio. No olvide que, en lugar de escribir el símbolo '@' en el nombre de correo electrónico, como se suele hacer, éste se sustituye por un punto cuando se coloca en el archivo de zonas.

Número de serie: El "número de versión" de este archivo de base de datos. Este número debería aumentar cada vez que cambie el archivo de base de datos.

Tiempo de actualización: El tiempo (en segundos) que esperará un servidor secundario entre comprobaciones de su servidor maestro para ver si el archivo de base de datos ha cambiado y si hay que pedir una transferencia de zona.

Tiempo de reintento: El tiempo (en segundos) que esperará un servidor secundario antes de volver a intentar una transferencia de zona que haya fallado.

Tiempo de caducidad: El tiempo (en segundos) que un servidor secundario seguirá intentando descargar una zona. Cuando haya pasado este tiempo, se rechazará la información antigua de la zona.

Tiempo de vida (TTL): El tiempo (en segundos) que un servidor DNS tiene permitido acumular en la caché cualquier registro del recurso de este archivo de base de datos.

Para que un registro de recurso abarque una línea en un archivo de base de datos, los saltos de línea deben incluirse entre paréntesis.

En un archivo de zona, el símbolo '@' representa el dominio raíz de la zona.

Ejemplo:

1; número de serie
10800; actualizar [3 horas]
3602; reintentar [1 hora]
604800; caducar [7 días]
86400; tiempo de vida [1 día]

REGISTRO NS

El Registro NS (Name Server o Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.

Su formato es el siguiente:

dominio IN NS nombreservidorhost

Ejemplos:

@ IN NS ns11.solo10.com.

@ IN NS ns12.solo10.com.

REGISTRO MX

El Registro de Intercambio de Correo (Mail eXchange) indica qué host procesa el correo de este dominio.

Si existen múltiples registros de intercambio de correo, intentará ponerse en contacto con los servidores de correo en orden de preferencia, empezando por los valores inferiores (mayor prioridad) hasta el valor superior (menor prioridad).

Su formato es el siguiente:

dominio IN MX preferencia servidorcorreohost

Al usar los siguientes registros de ejemplo, el correo enviado a prueba@midominio.com se envía primero a prueba@servidorcorreo0.midominio.com, si es posible, y luego a prueba@servidorcorreo1.midominio.com si servidorcorreo0 no está disponible.

Ejemplos:

@ IN MX 10 servidorcorreo0

@ IN MX 20 servidorcorreo1

El valor servidorcorreohost debe indicarse a través de un nombre y no de una dirección IP, ejemplo mail.midominio.com

REGISTRO A Y AAAA

Un Registro de dirección A (Address) sirve para asociar nombres de host a direcciones IP dentro de una zona. Éstos son los registros que componen la mayor parte del archivo DNS.

A = Address (Dirección) Este registro se usa para traducir nombres de hosts a direcciones Ipv4.

AAAA= Address (Dirección) Este registro se usa para traducir nombres de hosts a direcciones IPv6.

Su formato es el siguiente

dominio IN A direcciónIPdehost

Ejemplos:

www.solo10.com IN A 157.55.201.xxx
webmail IN A 157.55.200.xxx

El Registro CNAME

Estos registros también reciben el nombre de alias, aunque son conocidos como entradas de "nombre canónico" (CNAME o Canonical Name).

La utilidad principal de los mismos es la de usar más de un nombre para apuntar a un único host. Esto puede simplificar operaciones como albergar a la vez un servidor FTP y un webmail en el mismo equipo.

Su formato es el siguiente:

nombrealiashost IN CNAME nombrehost

Ejemplo:

Suponga que webmail.midominio.com y que ftp.midominio.com se encuentran en el mismo equipo. Si éste es el caso, entonces podría tener las siguientes entradas en su archivo de zona:

midominio.com IN A 157.55.200.xxx
ftp IN CNAME midominio.com
webmail IN CNAME midominio.com

REGISTROS PTR

Los registros 'PTR' o apuntadores, se usan para la resolución inversa. Por ejemplo, para hacer que 192.168.0.1 resuelva hacia www.sudominio.com. También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.

El registro debería verse como:

1.0.168.192.in-addr.arpa PTR www.sudominio.com.

Nota: La dirección IP se invierte en el primer campo. Recuerde poner el punto al final del nombre de host (segundo campo).

El método in-addr-arpa es el que se usa más a menudo.

Importante: Los registros 'PTR' solo son efectivos si su sitio tiene sus propias direcciones IP.

Importante: Los registros 'PTR' son solo efectivos si el archivo 'named.conf' se edita manualmente y se añade la información de zona pertinente. Esto solo puede hacerlo el usuario 'root' (el administrador del servidor).

Registros SPF

Sender Policy Framework - Ayuda a combatir el Spam. En este registro se especifica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe consulta el SPF para comparar la IP desde la cual le llega, con los datos de este registro.

Ejemplo:

midominio.com. IN TXT "v=spf1 mx ptr ~all"

En el ejemplo se indica un registro de texto (IN TXT) para el dominio midominio.com con la siguiente descripción SPF:

v= define la versión usada de SPF (versión 1).

mx autoriza a las máquinas con la IP de los registros MX.

Ptr autoriza a las máquinas bajo el dominio midominio.com.

~all sugiere desautorización a las máquinas que no encajen en lo autorizado explícitamente.

<https://www.solo10.com/kb/questions/114/>