Engineer

DNS

directorio que convierte un nombre en una dirección

Qué es

DNS, Domain Name System, es el directorio distribuido que consulta internet antes de que ocurra casi cualquier otra cosa. Un programa que tiene un nombre como `example.com` le pregunta a qué dirección conectarse, y el mismo sistema responde a otras preguntas sobre ese nombre: qué servidores aceptan su correo, qué texto ha publicado su propietario y qué servidores son responsables de él.

El directorio es un árbol que se lee de derecha a izquierda. Arriba está la raíz; debajo, dominios de nivel superior como `.com` o `.dk` ; después, los dominios que se registran y, debajo de ellos, los subdominios que crean sus propietarios. Ningún servidor contiene todo el árbol. Cada nivel delega la responsabilidad del siguiente en servidores identificados por su nombre. La parte del árbol de la que responde un conjunto de servidores se llama zona. Quien controla una zona decide a qué se resuelven sus nombres.

Dos tipos de servidores hacen el trabajo. Los autoritativos contienen una zona y responden por ella con la última palabra. Los resolutores recursivos, gestionados por proveedores de internet, empresas o servicios abiertos al público, recorren el árbol en nombre del cliente: preguntan a un servidor raíz dónde está `.com` , a `.com` dónde está `example.com` y a los servidores de ese dominio cuál es el registro, y devuelven la respuesta. El sistema operativo solo ejecuta un pequeño resolutor auxiliar, o stub, que pasa la pregunta a uno recursivo y espera.

Las respuestas son registros con un tipo definido, y el archivo de zona es la forma clásica de escribirlos:

```
$ORIGIN example.com.
$TTL 3600
@     IN  SOA    ns1.example.net. hostmaster.example.com. (
```

```
                2026101701 7200 900 1209600 300 )
@     IN  NS     ns1.example.net.
@     IN  A      192.0.2.10
@     IN  AAAA   2001:db8::10
www   IN  CNAME  example.com.
@     IN  MX     10 mail.example.net.
@     IN  TXT    "v=spf1 include:_spf.example.net -all"
```

`A` y `AAAA` proporcionan direcciones IPv4 e IPv6. `CNAME` convierte un nombre en alias de otro. `MX` identifica el servidor que recibe el correo y `TXT` transporta texto libre, que en la práctica incluye políticas de autenticación del correo y pruebas del control de un dominio. `NS` y `SOA` describen la propia zona.

Cada registro tiene un tiempo de vida, aquí de 3.600 segundos, y esa cifra es la clave del comportamiento de DNS. Un resolutor que ha obtenido una respuesta puede reutilizarla hasta que caduque su TTL, sin volver a preguntar. El resultado es un sistema que responde a la mayoría de las consultas desde una caché cercana al cliente y sigue respondiendo cuando un servidor autoritativo resulta brevemente inaccesible. El precio es que nadie puede obligar al mundo a olvidar antes de tiempo una respuesta antigua.

Utilice el concepto en una decisión

Aplique «¿Qué es DNS?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Wi-Fi, cortafuegos y acceso remoto configurados para trabajar desde cualquier lugar y permitir el acceso solo a las personas autorizadas.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. Administración de 30 VPS Ubuntu Linux — 30 servidores Linux administrados con recuperación planificada

Administración de 30 VPS Ubuntu Linux Póngase en contacto →

Por qué importa

Toda conexión a un servicio identificado por su nombre empieza con una consulta. Cuando DNS está mal, los servidores pueden estar perfectamente y, aun así, el sitio, la API y el correo parecen caídos porque nada llega hasta ellos. Cuando está bien, nadie lo nota; por eso suele ser la parte menos documentada de un sistema.

DNS también es donde se ejerce y demuestra el control de un dominio. Los proveedores de correo leen las políticas SPF, DKIM y DMARC en registros `TXT` para decidir si un mensaje que afirma proceder de su dominio es auténtico. Un

registro incorrecto o ausente envía, por tanto, correo legítimo a la carpeta de spam. Las autoridades de certificación y los servicios alojados piden un registro con un valor concreto como prueba de que el nombre le pertenece. Cualquiera que pueda editar la zona puede redirigir el sitio, interceptar el correo y obtener certificados para el dominio, lo que hace que el acceso a la cuenta DNS sea tan delicado como el acceso a los servidores.

La caché condiciona cada cambio. Lo que se llama propagación consiste, en realidad, en miles de resolutores que esperan a que caduque su propia copia. Para trasladar un sitio con pocas interrupciones, se reduce el TTL aproximadamente un día antes, se espera a que transcurra el TTL antiguo, se hace el cambio y se vuelve a aumentar el TTL cuando se haya estabilizado.

El DNS clásico viaja en texto sin cifrar, y ni las respuestas ni las preguntas son privadas. DNSSEC permite al resolutor comprobar que una respuesta procede realmente del propietario de la zona y no se ha modificado; su propia especificación indica que no aporta confidencialidad. Los transportes cifrados, como DNS sobre HTTPS, ocultan las preguntas a quienes observan el trayecto de red, pero el resolutor del otro extremo sigue viendo todos los nombres consultados. Elegir un resolutor es elegir quién recibe esa lista.

Cómo se aplica en la práctica

La zona de la propia empresa muestra el punto de partida más común y una forma de salir de él. Tenía unos veinte registros guardados en la consola web de un proveedor: la presencia web, un subdominio de git, dos redirecciones personales, correo dirigido a través de un proveedor de buzones alojados, un dominio de envío transaccional y los registros de autenticación de ambos. En una consola, el estado actual es lo que dejó la última persona que hizo clic. Ahora la zona son datos en un repositorio: registros en servicio, registros de aplicaciones, registros de políticas de transporte y una lista separada de registros pendientes de eliminar. Un play concilia esa declaración con la API del proveedor. Otros dos puntos de entrada requieren etiquetas de activación explícita: una auditoría que informa de las diferencias sin cambiar nada y una exportación que escribe la zona en el formato estándar de archivo de zona, para que pueda leerla algo más que el repositorio. La auditoría es lo más utilizado, porque se suele querer conocer la diferencia más a menudo que eliminarla.

El mismo proveedor tiene una función deliberadamente limitada. La página de créditos explica que Cloudflare atiende las consultas DNS del sitio y no hace nada más, sin un proxy delante, y muestra directamente la dirección del servidor: DNS ya la entrega a cualquiera que la pregunte.

Leer DNS también forma parte de la descripción rutinaria del conjunto de sistemas. Entre los siete roles de informes de solo lectura que documentan en Markdown el host en funcionamiento hay un inventario de proveedores que lee DNS junto con dos API de nube y una API de servidor dedicado, bajo la regla de que ningún informe muestre una cifra que su ejecución no haya medido.

Dónde surgen los problemas

Los fallos de DNS suelen llegar con retraso, quedar en caché o afectar a unos usuarios y a otros no. Por eso el mismo nombre funciona para una persona y falla para otra. Estos son los casos que se repiten.

Un cambio se resiste a aplicarse. Alguien edita un registro con un TTL de un día y espera que la nueva dirección surta efecto al instante, pero los resolutores que guardaron la respuesta antigua siguen sirviéndola hasta que caduca su copia. Una variante más discreta afecta a nombres nuevos: si se consultó un nombre antes de que existiera su registro, también se guarda en caché la respuesta negativa durante el tiempo que permita el `SOA` de la zona (RFC 2308). Reduzca los TTL antes de los cambios previstos y cree los registros antes de que algo los consulte.

Un alias ocupa un lugar que no le corresponde. RFC 1034 indica que un nombre con `CNAME` no puede contener ningún otro dato. El propio `example.com`, sin ningún prefijo de subdominio, siempre tiene registros `SOA` y `NS`. Por tanto, una zona que respete los estándares no puede convertir el vértice de la zona en alias; un `CNAME` en un subdominio que también necesita `MX` o `TXT` incumple la misma regla. Los proveedores ofrecen registros aplanados o `ALIAS` como solución propia; cada uno se comporta de forma algo distinta, así que lea qué sirve realmente el suyo.

La autenticación del correo se desborda. Cada `include` de un registro SPF provoca consultas DNS, y RFC 7208 limita el total a diez. Añadir otro servicio de boletines o de gestión de tickets puede superar el límite. Los receptores tratan entonces la política como un error permanente y juzgan sin ella el correo que debía autenticar. Cuente las consultas cada vez que añada un remitente.

Un registro sobrevive a su destino. Un subdominio apunta mediante `CNAME` a un bucket de almacenamiento en la nube o una aplicación alojada que se ha eliminado. Si el proveedor permite que cualquiera reclame ese nombre de recurso, un tercero puede hacerlo y servir contenido propio bajo el subdominio que usted dejó apuntando a ese recurso, con la reputación de su dominio asociada. Elimine el registro en el mismo cambio que elimina aquello a lo que apunta.

La zona solo existe en una consola. No hay historial, revisión ni diff, por lo que una eliminación accidental del registro `MX` se descubre cuando deja de llegar correo, y hay que reconstruir de memoria el valor anterior. Exportar la zona periódicamente o, mejor aún, declararla como código proporciona un registro de cada cambio y una forma de volver atrás.

Lecturas adicionales

- RFC 1035: nombres de dominio, implementación y especificación — Los formatos de los registros, la sintaxis del archivo de zona y el protocolo de transmisión.
- RFC 1034: nombres de dominio, conceptos y funcionalidades — El árbol, las zonas, la delegación y cómo los recorren los resolutores.
- RFC 9499: terminología de DNS — Definiciones precisas de las palabras utilizadas en esta página.
- RFC 2308: caché negativa de consultas DNS — Cuánto tiempo puede recordar un resolutor que un nombre no existe.
- RFC 4033: introducción y requisitos de seguridad de DNS — Qué protege DNSSEC y qué deja fuera.
- RFC 8484: consultas DNS sobre HTTPS — Consultas transportadas dentro del tráfico web cifrado corriente.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es DNS?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/dns/