

12.5. Características avanzadas de BIND

La mayoría de las implementaciones BIND solamente utilizan `named` para proporcionar servicios de resolución de nombres o para actuar como una autoridad para un dominio particular o sub-dominio. Sin embargo, BIND versión 9 tiene un número de características avanzadas que permiten un servicio DNS más seguro y avanzado.



Atención

Algunas de estas propiedades avanzadas, tales como DNSSEC, TSIG e IXFR (las cuales se definen en la sección siguiente), solamente se deberían usar en los entornos de red que tengan servidores de nombres que soporten estas propiedades. Si su entorno de red incluye servidores de nombres no-BIND o versiones anteriores de BIND, verifique que cada característica avanzada sea soportada antes de intentar utilizarla.

Todas las propiedades citadas aquí se describen en detalle en el **Manual de referencia para el administrador de BIND 9** referenciado en la [Sección 12.7.1](#).

12.5.1. Mejoras al protocolo DNS

BIND soporta Transferencias de zona incremental (Incremental Zone Transfers, IXFR), donde un servidor de nombres esclavo sólo descargará las porciones actualizadas de una zona modificada en un servidor de nombres maestro. El proceso de transferencia estándar requiere que la zona completa sea transferida a cada servidor de nombres esclavo hasta por el cambio más pequeño. Para dominios muy populares con archivos de zona muy largos y muchos servidores de nombres esclavos, IXFR hace que la notificación y los procesos de actualización sean menos exigentes en recursos.

Observe que IXFR solamente está disponible cuando utiliza la *actualización dinámica* para realizar los cambios en los registros de zona maestra. Si cambia los archivos de zona manualmente, tiene que usar AXFR (Automatic Zone Transfer). Encontrará más información sobre la actualización dinámica en el **Manual de referencia para el administrador de BIND 9**. Consulte la [Sección 12.7.1](#) para más información.

12.5.2. Vistas múltiples

A través del uso de la declaración `view` en `named.conf`, BIND puede presentar información diferente dependiendo desde cuál red se esté realizando la petición.

Esto es básicamente usado para negar entradas DNS confidenciales a clientes fuera

de la red local, mientras se permiten consultas desde clientes dentro de la red local.

La declaración `view` usa la opción `match-clients` para coincidir direcciones IP o redes completas y darles opciones especiales y datos de zona.

12.5.3. Seguridad

BIND soporta un número de métodos diferentes para proteger la actualización y zonas de transferencia, en los servidores de nombres maestro y esclavo:

- *DNSSEC* — Abreviación de *DNS SECurity*, esta propiedad permite firmar con caracteres criptográficos zonas con una *clave de zona*.

De esta manera, puede verificar que la información de una zona provenga de un servidor de nombres que la ha firmado con caracteres criptográficos con una clave privada, siempre y cuando el recipiente tenga esa clave pública del servidor de nombres.

BIND versión 9 también soporta el método SIG(0) de llave pública/privada de autenticación de mensajes.

- *TSIG* — Abreviación para *Transaction SIGnatures*, esta característica permite una transferencia desde el maestro al esclavo sólo después de verificar que una llave secreta compartida existe en ambos servidores maestro y en el esclavo.

Esta característica fortalece el método estándar basado en direcciones IP de transferencia de autorización. Un intruso no solamente necesitará acceso a la dirección IP para transferir la zona, sino también necesitará conocer la clave secreta.

BIND versión 9 también soporta *TKEY*, el cual es otro método de autorización de zonas de transferencia basado en clave secreta compartida.

12.5.4. IP versión 6

BIND versión 9 puede proporcionar servicios de nombres en ambientes IP versión 6 (IPv6) a través del uso de registros de zona `A6`.

Si el entorno de red incluye hosts IPv4 e IPv6, use el demonio ligero de resolución `lwresd` en todos los clientes de la red. Este demonio es muy eficiente, funciona solamente en caché y además entiende los nuevos registros `A6` y `DNAME` usados bajo IPv6. Consulte la página de manual para `lwresd` para más información.

[Anterior](#)

Uso de `rndc`

[Inicio](#)

[Subir](#)

[Siguiente](#)

Errores comunes que debe evitar