12.4. Uso de `rndc`

BIND incluye una utilidad llamada `rndc` la cual permite la administración de línea de comandos del demonio `named` desde el host local o desde un host remoto.

Para prevenir el acceso no autorizado al demonio `named`, BIND utiliza un método de autenticación de llave secreta compartida para otorgar privilegios a hosts. Esto significa que una llave idéntica debe estar presente en los archivos de configuración `/etc/named.conf` y en el `rndc`, `/etc/rndc.conf`.

12.4.1. Configuración de `/etc/named.conf`

Para que `rndc` se pueda conectar a un servicio `named`, debe haber una declaración `controls` en el archivo de configuración del servidor BIND `/etc/named.conf`.

La declaración `controls` mostrada abajo en el ejemplo siguiente, permite a `rndc` conectarse desde un host local.

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { <key-name>; };
};
```

Esta declaración le dice a `named` que escuche en el puerto por defecto TCP 953 de la dirección loopback y que permita comandos `rndc` provenientes del host local, si se proporciona la llave correcta. El valor *<key-name>* especifica un nombre en la declaración `key` dentro del archivo `/etc/named.conf`. El ejemplo siguiente ilustra la declaración `key`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

En este caso, el *<key-value>* utiliza el algoritmo HMAC-MD5. Utilice el comando siguiente para generar llaves usando el algoritmo HMAC-MD5:

```
dnssec-keygen -a hmac-md5 -b <bit-length> -n HOST <key-file-name>
```

Una llave con al menos un largo de 256-bit es una buena idea. La llave que debería ser colocada en el área *<key-value>* se puede encontrar en el archivo *<key-file-name>* generado por este comando.

Aviso

Debido a que `/etc/named.conf` está accesible a todo el mundo, es una buena idea colocar la declaración `key` en un archivo separado que sólo esté accesible por root y luego utilizar una declaración `include` para referenciarlo. Por ejemplo:

```
include "/etc/rndc.key";
```

12.4.2. Configuración de `/etc/rndc.conf`

La declaración `key` es la más importante en `/etc/rndc.conf`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

<key-name> y *<key-value>* deberían ser exáctamente los mismos que sus configuraciones en `/etc/named.conf`.

Para coincidir las claves especificadas en el archivo de configuración del servidor objetivo `/etc/named.conf`, agregue las líneas siguientes a `/etc/rndc.conf`.

```
options {
  default-server  localhost;
  default-key     "<key-name>";
};
```

Este directriz configura un valor de llave global por defecto. Sin embargo, el archivo de configuración `rndc` también puede usar llaves diferentes para servidores diferentes, como en el ejemplo siguiente:

```
server localhost {
  key  "<key-name>";
};
```

Atención

Asegúrese de que sólo el usuario root pueda leer y escribir al archivo `/etc/rndc.conf`.

Para más información sobre el archivo `/etc/rndc.conf`, vea la página man de `rndc.conf`.

12.4.3. Opciones de línea de comandos

Un comando `rndc` toma la forma siguiente:

```
rndc <options> <command> <command-options>
```

Cuando esté ejecutando `rndc` en una máquina local configurada de la forma correcta, los comandos siguientes están disponibles:

- `halt` — Para inmediatamente el servicio named.
- `querylog` — Registra todas las peticiones hechas a este servidor de nombres.
- `refresh` — Refresca la base de datos del servidor de nombres.
- `reload` — Recarga los archivos de zona pero mantiene todas las respuestas precedentes situadas en caché. Esto le permite realizar cambios en los archivos de zona sin perder todas las resoluciones de nombres almacenadas.

  Si los cambios sólo afectaron una zona específica, vuelva a cargar solamente esa una zona específica añadiendo el nombre de la zona después del comando `reload`.
- `stats` — Descarga las estadísticas actuales de `named` al archivo `/var/named/named.stats`.
- `stop` — Detiene al servidor salvando todas las actualizaciones dinámicas y los datos de las *Transferencias de zona incremental* (*IXFR*) antes de salir.

Ocasionalmente, puede ser necesario ignorar las configuraciones por defecto en el archivo `/etc/rndc.conf`. Estan disponibles las siguientes opciones:

- `-c <configuration-file>` — Especifica la ubicación alterna de un archivo de configuración.
- `-p <port-number>` — Especifica la utilización de un número de puerto diferente del predeterminado 953 para la conexión del comando `rndc`.
- `-s <server>` — Especifica un servidor diferente al `default-server` listado en `/etc/rndc.conf`.
- `-y <key-name>` — Le permite especificar una llave distinta de la opción `default-key` en el archivo `/etc/rndc.conf`.

Se puede encontrar información adicional sobre estas opciones en la página del manual de `rndc`.

Archivos de zona Subir Características avanzadas de BIND