

Network Time Protocol

1. Introducción

El Network Time Protocol (NTP) se usa para sincronizar la hora de una computadora cliente o servidora a la hora de otra máquina servidora o a una fuente de referencia, a través de un receptor radio o una conexión vía satélite o módem. La exactitud que proporciona depende de la si la red es una LAN, en cuyo caso tendremos una precisión de milisegundos, o una WAN, en la que el retardo se incrementa en unas decenas de milisegundos.

Típicamente, las configuraciones de NTP utilizan tanto servidores como caminos redundantes, proporcionando así exactitud y fiabilidad. Inclusive algunas configuraciones permiten autenticación para prevenir ataques accidentales o maliciosos al protocolo.

NTP soporta tanto sistemas Unix como los basados en Windows (NT 4.0 y 2000). El procedimiento de instalación del servidor presenta cierta diversidad de procedimientos que permiten compilar la distribución e instalarla en un típico cliente o servidor. El procedimiento de instalación inspecciona el hardware del sistema y también el software y selecciona automáticamente las opciones más convenientes para ese entorno.

Crear un servidor primario requiere un receptor radio, satélite o un módem. Sin embargo, también es posible configurar una máquina en una red aislada con un controlador de reloj y tener otras máquinas sincronizadas con ella.

NTP es una aplicación de red distribuida que puede ser utilizada en muy diversos escenarios, aunque la mayor parte de los mismos sólo utilizarán una pequeña parte de los mismos requerirán sólo unas cuantas de estas facilidades. Para conseguir fiabilidad y exactitud es necesario preparar un archivo de configuración adecuado, comúnmente llamado `/etc/ntp.conf`, que establezca los servidores y/o receptores externos o módems más adecuados que se puedan utilizar. Más tarde entraremos en la creación de este archivo.

NTP soporta, además, la creación de una “subred” redundante de servidores y clientes organizados en distintos estratos según sea su cometido. Los servidores primarios operan en el primer estrato y proporcionan sincronización a los servidores que se encuentran en el segundo y estos a su vez a los que se encuentran en el siguiente, y así sucesivamente. En este tipo de jerarquía los clientes son simplemente servidores que no tienen otros servidores que dependan de ellos. La subred NTP incluye en la actualidad aproximadamente un centenar de servidores primarios (estrato 1) sincronizados directamente a UTC (coordinated universal time) por radio, satélite o módem. Normalmente las estaciones de trabajo y servidores con pocos clientes no se sincronizan con servidores primarios directamente. Hay aproximadamente un centenar de servidores públicos secundarios (estrato 2) sincronizados a los servidores primarios y que proporcionan sincronización a un total de más de 100 000 clientes y servidores de Internet.

2.NTPD

El programa `ntpd` es un servidor demonio que establece y mantiene la hora del sistema en sincronismo con los servidores de hora estándares en Internet. Es una implementación completa del NTP (Network Time Protocol) versión 4, aunque mantiene compatibilidad con las versiones anteriores (3, 2 y 1), definidas respectivamente en las RFC's 1305, 1059 y 1119.

Ntpd realiza la mayoría de los cálculos en aritmética de punto flotante, con una precisión de 232 picosegundos. Sin embargo, esta precisión no es alcanzable con estaciones de trabajo ordinarias y las redes de comunicaciones de nuestros días, si bien en un futuro no muy lejano puede llegar a alcanzarse gracias al incremento en velocidad de las CPU's y a las redes locales de alta velocidad.

Sinopsis

```
ntpd [ -aAbdgLmNPqx ] [ -c conffile ] [ -f driftfile ] [ -g ] [ -k keyfile ] [ -l logfile ] [ -N high ]  
[ -p pidfile ] [ -r broadcastdelay ] [ -s statsdir ] [ -t key ] [ -v variable ] [ -V variable ] [ -x ]
```

Funcionamiento de NTP

El funcionamiento de `ntpd` está basado en el intercambio de mensajes con todos aquellos servidores que se hayan configurado en el fichero `/etc/ntp.conf` y con un determinado intervalo de tiempo entre las sucesivas consultas. Al arrancar el programa este requiere el intercambio de distintos mensajes con la mayoría de los servidores configurados, de forma que los diferentes algoritmos puedan acumular datos y de esta forma establecer la hora en el reloj. Para proteger a la red de ráfagas de mensajes, el intervalo inicial de intercambio de los mismos se retrasa un intervalo de tiempo aleatorio entre 0 y 16 segundos (este retardo inicial puede ser reducido mediante la opción *iburst* del comando de configuración del servidor). Teniendo en cuenta que inicialmente el intervalo por defecto de intercambio de mensajes es de 64 segundos, pueden pasar varios minutos hasta que la hora del reloj quede configurada.

La mayoría de los sistemas operativos y el hardware actual incorporan un chip time-of-year (TOY) para mantener la hora durante los periodos en los que la máquina está apagada. Cuando esta es arrancada, el chip se utiliza para inicializar la hora del sistema operativo. Posteriormente la máquina se sincroniza con un servidor NTP y es sistema operativo, en función de la información recabada, se encarga de corregir la hora del chip de cuando en cuando. Caso de que no exista TOY o que la diferencia entre la hora de este y del servidor NTP supere los 1000 segundos habrá de ser el propio operador quien proceda a cambiar la hora manualmente, salvo que se especifique en el comando la opción `-g`, que hace que se ignore este hecho y por lo tanto se ponga en el TOY la hora del servidor. Si después de modificar la hora del TOY se vuelve a detectar una diferencia mayor de 1000 segundos entre ambos relojes, `ntpd` terminará la ejecución y saldrá con un mensaje de pánico a un fichero de log.

Generalmente NTP ajusta la hora en pequeños saltos, de forma que no aparezcan grandes discontinuidades. Sin embargo, en situaciones en las que la congestión en la red es elevada, el retardo puede ser mayor de tres segundos. En general, los algoritmos de `ntpd` descartan toda muestra que exceda un retardo de 128 ms, salvo que el tiempo durante el cual no se reciben muestras con retardo menor de 128ms sea superior a 900s, en cuyo caso sí se aceptan estas tramas como válidas.

Comportamiento de Ntpd

El comportamiento del demonio ntpd en el arranque depende de la existencia o no del fichero ntp.drift. Este fichero contiene la última estimación de error de frecuencia, o lo que es lo mismo, en la dispersión en la llegada de las muestras. Cuando este fichero no existe, el ntpd entra en un modo especial en el que se busca la adaptación a la hora del servidor y establecer el error de frecuencia que tendremos. Este proceso lleva aproximadamente 15 minutos, después de los cuales la hora y frecuencia se establecen a sus valores nominales y ntpd entra en modo normal, donde tanto la frecuencia como el tiempo son monitorizados. Después de una hora se crea el fichero ntp.drift, que albergará el dato de error de frecuencia. Si por el contrario al arrancar el demonio ntpd este fichero ya existe, la frecuencia de ntpd se inicializa directamente desde el fichero y entra inmediatamente en modo normal, actualizándose de forma horaria el contenido de dicho fichero en función de los datos recibidos.

Modos de operación

Ntpd puede operar en distintos modos: pasivo/activo, cliente/servidor con broadcast/multicast. Sin embargo, la configuración más típica consiste en la monitorización continua de los pequeños cambios que se puedan producir en la frecuencia y hora del reloj para conseguir de este modo la mayor precisión posible. Sin embargo, puede operar en un modo en el cual la hora la establece un servidor externo y la frecuencia se obtiene de un fichero previamente creado. Un cliente broadcast/multicast puede descubrir servidores remotos, calcular con posterioridad los retardos de propagación entre ellos y configurarse automáticamente.

Por defecto ntpd se ejecuta en modo continuo, donde cada uno de los posibles servidores externos es interrogado a intervalos utilizando para ello un algoritmo heurístico, cuya misión es la de encontrar el mejor intervalo de interrogación con el que podemos preguntar al servidor. Es habitual que inicialmente las interrogaciones se produzcan cada 64 segundos y, eventualmente, cada 1024 segundos.

En algunos casos, puede ser una buena opción la de que ntpd no se encuentre ejecutándose continuamente, sino que es una opción bastante típica la de ejecutar el programa ntpdate como un trabajo del cron cada determinado tiempo.

Control de los intervalos de sondeo

En general, las implementaciones de NTP existentes han de tener dos características. En primer lugar deben tener una máquina de estado que permita reducir la carga que soporta la red, y como segundo aspecto dicha máquina de estados permita mantener una sincronización adecuada. En general, ambos aspectos están reñidos, de forma que cuando lo que prima es una buena sincronización se reduce el intervalo de sondeo, mientras que si lo importante es reducir la sobrecarga de la red lo habitual es aumentarlo.

Sin embargo, es importante analizar las consecuencias que puede acarrear el hecho de cambiar el intervalo de sondeo desde su valor mínimo de 64 segundos hasta el valor máximo de 1024 segundos. La mayoría de los controladores de dispositivo no funcionan adecuadamente si el sondeo se produce con una periodicidad menor de 64 segundos, además de que tanto el servidor de broadcast y los clientes manycast utilizan habitualmente valores por defecto. En general, cuando la actualización del reloj se estabiliza el intervalo se incrementará desde el valor mínimo hasta el valor máximo.

Configuración básica de NTPD

La configuración básica de ntpd aquella que puede ser utilizada por el 90% de los usuarios de ntpd. Esta configuración solamente necesita un reloj de referencia, al que se direcciona en xntpd mediante una pseudo-dirección IP. Por lo tanto, el archivo de configuración /etc/ntp.conf podría tener un aspecto como el siguiente:

```
server 127.127.8.0 mode 5    # GENERIC DCF77 AM
```

Adicionalmente a esta configuración minimalista se le podría añadir otros datos de configuración, como por ejemplo un drift-file, servidores adicionales, configuración y monitorización remota, restricciones de acceso, etc.

A pesar de su sencillez y funcionalidad, esta configuración no es demasiado típica. La mayoría de los servidores de NTP no tienen relojes de referencia, sino que usan servidores de estratos inferiores como referencias temporales. Este tipo de

servidores se pueden encontrar en la página de Internet de NTP. El archivo de configuración no varía prácticamente nada:

```
server 132.199.176.10 # Dirección IP del servidor de NTP
```

Además hemos de tener en cuenta que si configuramos múltiples servidores tendremos un ajuste de tiempo mucho más exacto. Esto se debe a que NTP es capaz de seleccionar los mejores servidores de entre los proporcionados.

¿Cuál es la Pseudo dirección IP de mi reloj de referencia?

Los diferentes controladores de los relojes de referencia se seleccionan usando direcciones IP, ya que el convenio de nomenclatura de los mismos establece que el formato de dirección es el siguiente: cuatro bytes separados por puntos, de los cuales los dos primeros son 127, 127 y les sigue el Tipo de Reloj y Número de Unidad. Además es posible configurar distintos relojes simultáneamente, ya que el controlador mapea los diferentes números de unidad en uno o más archivos de dispositivo. Los relojes soportados y los correspondientes ficheros de configuración están listados en la página oficial de NTP (refclock.html y drivern.html).

¿ Qué es un "drift-file"?

Cuando xntpd está ejecutándose trata de averiguar la deriva del reloj del sistema con respecto al reloj de referencia. Para que xntpd pueda conocer en qué medida existía deriva entre los dos relojes durante la última ocasión en que estuvo activo, esta se guarda en el fichero `/etc/ntp.drift`, de manera que al arrancar de nuevo lee este fichero y así consigue una rápida convergencia entre los valores del reloj local y del servidor. Para ello se ha de poner lo siguiente en el fichero de configuración:

```
driftfile /etc/ntp.drift
```

Por último, aclararemos algo las opciones de línea de comandos para el comando `ntpd` que expusimos al comienzo:

- a Es una opción por defecto que permite autenticación.
- A Inhabilita la autenticación.

-b Sincronización a través de mensajes de broadcast a todos los servidores.

-c conffile Especifica nombre y lugar del archivo de configuración.

-f driftfile Especifica nombre y lugar del archivo de configuración.

-k keyfile Especifica nombre y lugar del archivo de configuración.

-l logfile Especifica nombre y lugar del archivo de configuración.

-s statsdir Especifica el directorio donde se almacenan las estadísticas.

-t key Añade una nueva clave a la lista de claves.