Mise en place d'une synchronisation des horloges via NTP

Jean-Philippe DURAND

30 janvier 2006

Présentation

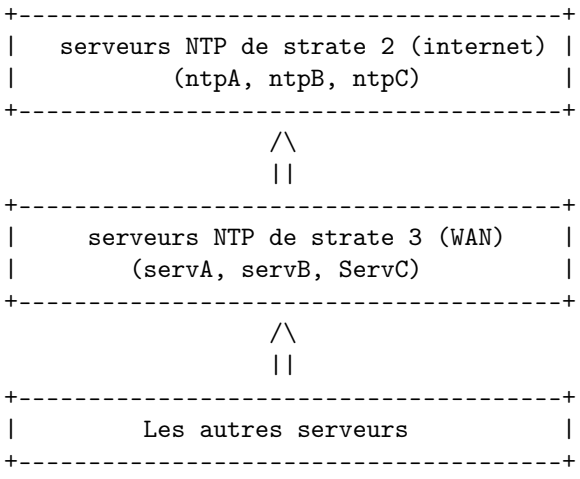
Avec le temps, l'horloge d'un ordinateur tend à dériver. Le protocole NTP («Network Time Protocol») est une des manières pour s'assurer que l'horloge reste précise.
De nombreux services Internet ont besoin, ou tirent partie, de la précision des horloges des ordinateurs. Par exemple, un serveur web, peut recevoir des requêtes pour n'envoyer un fichier que s'il a été modifié depuis un certain temps. Sur un réseau local, il est essentiel que les ordinateurs partageant des fichiers à partir du même serveur de fichiers aient des horloges synchronisées de manière à ce que les dates de création ou de dernière modification d'un fichier («timestamp») soient cohérentes. Des services comme `cron` reposent sur une horloge système précise pour exécuter des commandes à des moments précis. La désynchronisation des horloges des serveurs a pour conséquence:

- des problèmes de suivi des logs (les dates/heures sont erronées),
- des problèmes de téléscopage de jobs lancés la nuit,
- des problèmes d'horodatage des mails,
- *etc.*

Pour maintenir à l'heure un ensemble de serveurs on utilise le protocole NTP.

Architecture retenue

Choisir plusieurs serveurs NTP non-connectés entre eux est une bonne idée au cas où un des serveurs utilisé devient inaccessible ou que son horloge n'est plus fiable. `ntpd` utilise intelligemment les réponses qu'il reçoit d'autres serveurs –il favorise les plus fiables par rapport aux moins fiables.



`WAN = 172.16.0.0/16`

servA = 172.16.1.1
servB = 172.16.1.2
servC = 172.16.1.3
Si un serveur des strates 2 ou 3 est indisponible, les serveurs de la strate N+1 se synchroniseront avec les serveurs restants.

Mise en place d'un serveur NTP sous linux

On peut ne synchroniser l'horloge uniquement lors du démarrage de la machine, en employant `ntpdate`. Cela peut être approprié pour certaines machines de bureau qui sont fréquemment rédémarrées et qui ne nécessite qu'une synchronisation épisodique, cependant la plupart des machines devraient utiliser `ntpd`.
Utiliser `ntpdate` au moment du démarrage est également une bonne idée pour les machines qui exécutent `ntpd`. Le programme `ntpd` modifie l'horloge graduellement, alors que `ntpdate` change directement l'horloge, peu importe la différence entre l'heure actuelle de la machine et l'heure correcte.
Pour activer `ntpdate` au démarrage, ajoutez la ligne `ntpdate_enable="YES"` au fichier `/etc/rc.conf`.
Préciser également tous les serveurs avec lesquels on veut se synchroniser et tous les indicateurs devant être passés à `ntpdate` avec `ntpdate_flags`.
Le serveur NTP est déjà installé par défaut, il faut juste le paramétrer, ci-après un exemple de `ntp.conf` :

```
# tout en deny all par defaut
restrict default ignore

# on autorise les ips ci-dessous (clients)
restrict 127.0.0.1
restrict 172.16.0.0 mask 255.255.0.0 notrust nomodify notrap

# on autorise et on declare les serveurs ntp stratum 2
server <ip servA> prefer
server <ip servB>
server <ip servC>
restrict <ip servA> mask 255.255.255.255 nopeer nomodify notrap noquery
restrict <ip servB> mask 255.255.255.255 nopeer nomodify notrap noquery
restrict <ip servC> mask 255.255.255.255 nopeer nomodify notrap noquery

# si aucune source NTP n'est disponible on utilise la local clock
server  127.127.1.0     # local clock
fudge   127.127.1.0 stratum 10

# divers
logfile /var/log/ntp.log
driftfile /etc/ntp/drift
authenticate no
```

Enfin, il suffit ensuite d'activer le service au démarrage dans la sequence de boot et de le lancer à la main pour la première fois sans redémarrer la machine, exécuter `ntpd` en étant sûr de préciser tout paramètre supplémentaire de `ntpd_flags` dans `/etc/rc.conf`. Par exemple:

```
# ntpd -p /var/run/ntpd.pid
```

Attention, l'heure du système ne doit pas être trop éloignée de l'heure réelle sinon `ntpd` refusera d'effectuer la synchronisation:

```
# ntpdate ntp.laas.fr
```

```
# hwclock --systohc
# chkconfig ntpd on
# /etc/init.d/ntpd start
```
L'option `server` précise quels serveurs doivent être utilisés, avec un serveur listé par ligne. Si un serveur est spécifié avec l'argument `prefer`, comme c'est le cas pour servA, ce serveur est préféré par rapport aux autres serveurs. Une réponse en provenance d'un serveur préféré sera ignorée si elle diffère de façon significative des réponses des autres serveurs, sinon elle sera utilisée sans considérer les autres réponses. L'argument `prefer` est normalement employé pour les serveurs NTP qui sont connus pour leur grande précision, comme ceux avec des systèmes spéciaux de contrôle du matériel.
L'option `driftfile` précise quel fichier est utilisé pour stocker le décalage de fréquence de l'horloge. Le programmme `ntpd` l'utilise pour compenser automatiquement la dérive naturelle de l'horloge, permettant de maintenir un réglage raisonnablement correct même s'il est coupé d'autres sources extérieures de temps pendant une certaine période.
L'option `driftfile` précise également quel fichier est utilisé pour stocker l'information concernant les réponses précédentes des serveurs NTP utilisés. Il ne devrait pas être modifié par un autre processus.
Par défaut, le serveur NTP sera accessible par toutes les machines sur l'Internet. L'option `restrict` du fichier `/etc/ntp.conf` permet de contrôler quelles machines peuvent accéder au serveur.
Si on veut refuser à tout le monde l'accès au serveur NTP, ajouter la ligne suivante au fichier `/etc/ntp.conf`:
`restrict default ignore`
Si on désire autoriser uniquement l'accès aux machines de son réseau local pour qu'elles puissent synchroniser leur horloge, tout en s'assurant qu'elles ne peuvent configurer le serveur ou être utilisées comme point de de synchronisation, ajouter:
`restrict 192.168.0.1 mask 255.255.255.0 nomodify notrap`
à la place, où `192.168.0.1` est une adresse IP du réseau local et `255.255.255.0` est le masque de sous-réseau.

Mise en place d'un client NTP sur un serveur W2K

Normalement, par défaut, le service est lancé automatiquement lors du boot, si ce n'est pas le cas, il faut penser à l'activer dans le gestionnaire de services:

```
> net time /setsntp:172.16.1.1,172.16.1.2,172.16.1.3
> net stop w32time
> net start w32time
```

La clé de registre du paramétrage de NTP est

```
> net time /setsntp:172.16.1.1,172.16.1.2,172.16.1.3
```

`\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControleSet\Services\W32Time\Parameters.`

Liste de serveurs NTP

Une liste de serveurs NTP accessibles par le public est disponible ici : `http://ntp.isc.org/bin/view/Servers/WebHome`.