

Dernière mise-à-jour : 2020/01/30 03:27

108.1 - Gestion de l'horloge système (3/60)

Le Serveur d'Horloge

Introduction

Dans le cas d'un serveur de réseau, il est souvent important de maintenir l'heure de la machine à l'heure exacte pour des raisons de simplification de synchronisation avec des portables ou bien des systèmes de fichiers externes. Pour accomplir cette tâche, nous utilisons les services de serveurs de temps publics disponibles sur Internet sur lesquels nous synchronisons l'horloge de notre serveur. De même, les machines de notre réseau peuvent se synchroniser ensuite avec l'heure de notre serveur.

Le protocole utilisé s'appelle **NTP** (**Network Time Protocol**) qui utilise le port **123**. Celui-ci, permet la synchronisation avec plusieurs serveurs publics. Les serveurs de temps de racine s'appellent des serveurs de **Strate 1**. En dessous se trouvent des serveurs de Strate 2, Strate 3 etc..

Installation

Sous CentOS, le serveur **ntpd** est normalement installé par défaut :

```
[root@centos6 ~]# rpm -qa | grep ntp
ntpdate-4.2.4p8-2.el6.i686
fontpackages-filesystem-1.41-1.1.el6.noarch
ntp-4.2.4p8-2.el6.i686
```

Par contre le service ntpd n'est pas démarré par défaut :

```
[root@centos6 ~]# chkconfig --list | grep ntpd
ntpd          0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
```

ntpd	0:arrêt	1:arrêt	2:arrêt	3:arrêt	4:arrêt	5:arrêt	6:arrêt
------	---------	---------	---------	---------	---------	---------	---------

Configurez le service **nptd** pour que celui-ci soit activé correctement pour les niveaux d'exécution 3, 4 et 5 :

```
[root@centos6 ~]# chkconfig --level 345 ntpd on
[root@centos6 ~]# chkconfig --list | grep ntpd
ntpd          0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
ntpd         0:arrêt    1:arrêt    2:arrêt    3:arrêt     4:arrêt     5:arrêt     6:arrêt
```



La commande **ntpdate**, utilisée pour synchroniser l'horloge **sans** utiliser le démon **ntpd** est maintenant remplacée par l'option **-q** de la commande **ntp**. Lors de l'utilisation de **ntpdate**, le démon **ntpd** doit être arrêté. Si **ntpdate** constatait que l'erreur de l'horloge local était supérieur à 0,5 secondes, celle-ci appelait la routine **settimeofday()** tandis que si l'erreur était inférieur à 0,5 secondes, elle appelait la routine **adjtime()**.

Le fichier **ntp.conf**

Le service **ntpd** est configuré par le fichier **/etc/ntp.conf** :

[ntp.conf](#)

```
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

```
# Permit all access over the loopback interface. This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org

#broadcast 192.168.1.255 autokey      # broadcast server
#broadcastclient                    # broadcast client
#broadcast 224.0.1.1 autokey         # multicast server
#multicastclient 224.0.1.1          # multicast client
#manycastserver 239.255.254.254      # manycast server
#manycastclient 239.255.254.254 autokey # manycast client

# Undisciplined Local Clock. This is a fake driver intended for backup
# and when no outside source of synchronized time is available.
#server 127.127.1.0      # local clock
#fudge 127.127.1.0 stratum 10

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
```

```
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
#statistics clockstats cryptostats loopstats peerstats
```

Les directives actives de ce fichier sont :

[ntp.conf.bare](#)

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
driftfile /var/lib/ntp/drift
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
includefile /etc/ntp/crypto/pw
keys /etc/ntp/keys
```

Afin de mieux comprendre les détails de ce fichier, nous passons en revue ces directives.

Les directives suivantes permettent la synchronisation avec notre source ntp mais interdisent à cette source de faire de requêtes à notre serveur ou de

modifier le service sur notre système :

```
restrict default kod nomodify notrap nopeer noquery  
restrict -6 default kod nomodify notrap nopeer noquery
```

Les directives suivantes permettent l'accès au serveur via l'interface loopback :

```
restrict 127.0.0.1  
restrict -6 ::1
```

Les directives suivantes stipulent quel serveur est utilisé pour la synchronisation. La liste peut aussi comporter des numéros IP:

```
server 0.rhel.pool.ntp.org  
server 1.rhel.pool.ntp.org  
server 2.rhel.pool.ntp.org
```



Les directives ci-dessus sont souvent suivies par deux options : **server 0.rhel.pool.ntp.org iburst dynamic**. L'option **iburst** implique qu'en cas de non-disponibilité du serveur concerné, votre serveur enverra des lots de 8 paquets au lieu d'un seul. L'option **dynamic** permet la configuration de votre serveur même dans le cas où le serveur NTP distant n'est pas disponible car l'utilisation de cette option présume que le serveur distant deviendra disponible à un moment donné.

Les directives suivantes stipulent que votre serveur doit se synchroniser sur l'horloge locale, une horloge fictive, utilisée lors de l'inaccessibilité des serveurs sur Internet :

```
server 127.127.1.0          # local clock  
fudge 127.127.1.0 stratum 10
```

Ces deux lignes étant en commentaire, il convient d'ôter les caractères **#** pour activer cette fonctionnalité.

La directive suivante identifie le fichier contenant la déviation moyenne:

```
driftfile /var/lib/ntp/drift
```

La directive suivante indique le répertoire qui stocke les clefs symétriques lors d'accès sécurisés éventuels :

```
keys /etc/ntp/keys
```

La directive suivante génère des statistiques dans le répertoire **/var/log/ntpstats** :

```
statistics clockstats cryptostats loopstats peerstats
```

Etant en commentaire, il convient d'ôter le caractère **#** pour activer les statistiques.

Pour créer un fichier d'historique, il convient d'ajouter la directive suivante :

```
logfile /var/log/xntpd
```

Votre fichier /etc/ntp.conf deviendra donc :

[ntp.conf](#)

```
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface. This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
```

```
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org

#broadcast 192.168.1.255 autokey      # broadcast server
#broadcastclient                     # broadcast client
#broadcast 224.0.1.1 autokey         # multicast server
#multicastclient 224.0.1.1           # multicast client
#manycastserver 239.255.254.254      # manycast server
#manycastclient 239.255.254.254 autokey # manycast client

# Undisciplined Local Clock. This is a fake driver intended for backup
# and when no outside source of synchronized time is available.
server 127.127.1.0    # local clock
fudge 127.127.1.0 stratum 10

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
```

```
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
statistics clockstats cryptostats loopstats peerstats

logfile /var/log/xntpd
```

Options de la commande

Les options de la commande ntpd sont :

```
[root@centos6 ~]# ntpd --help
ntpd - NTP daemon program - Ver. 4.2.4p8
USAGE: ntpd [ -<flag> [<val>] | --<name>[={| }<val>] ]...
  Flg Arg Option-Name      Description
  -4 no  ipv4              Force IPv4 DNS name resolution
  -6 no  ipv6              Force IPv6 DNS name resolution
                        - an alternate for ipv4
  -a no  authreq           Require crypto authentication
                        - prohibits these options:
                          authnreq
  -A no  authnreq          Do not require crypto authentication
                        - prohibits these options:
                          authreq
  -b no  bcastsync         Allow us to sync to broadcast servers
```

```
-c Str configfile      configuration file name
-d no  debug-level     Increase output debug message level
      - may appear multiple times
-D Str set-debug-level Set the output debug message level
      - may appear multiple times
-f Str driftfile       frequency drift file name
-g no  panicgate       Allow the first adjustment to be Big
-i Str jaildir         Jail directory
-I Str interface       Listen on interface
      - may appear multiple times
-k Str keyfile         path to symmetric keys
-l Str logfile         path to the log file
-L no  novirtualips    Do not listen to virtual IPs
-n no  nofork          Do not fork
-N no  nice            Run at high priority
-p Str pidfile         path to the PID file
-P Num priority        Process priority
-q no  quit            Set the time and quit
-r Str propagationdelay Broadcast/propagation delay
-U Num updateinterval interval in seconds between scans for new or dropped interfaces
-s Str statsdir        Statistics file location
-t Str trustedkey      Trusted key number
      - may appear multiple times
-u Str user            Run as userid (or userid:groupid)
-v Str var             make ARG an ntp variable (RW)
      - may appear multiple times
-V Str dvar           make ARG an ntp variable (RW|DEF)
      - may appear multiple times
-x no  slew           Slew up to 600 seconds
-m no  mlock          Lock memory
-v opt version        Output version information and exit
-? no  help           Display usage information and exit
-! no  more-help      Extended usage information passed thru pager
```

Options are specified by doubled hyphens and their name or by a single hyphen and the flag character.

The following option preset mechanisms are supported:

- examining environment variables named NTPD_*

please send bug reports to: <http://bugs.ntp.org>, bugs@ntp.org

Créez maintenant le fichier de journalisation :

```
[root@centos6 ~]# touch /var/log/xntpd
```

Ensuite modifiez le groupe associé à ce fichier :

```
[root@centos6 ~]# chgrp ntp /var/log/xntpd
```

Dernièrement modifiez les permissions sur le fichier de journalisation :

```
[root@centos6 ~]# chmod 664 /var/log/xntpd
```

LAB #1



Modifiez votre fichier `ntp.conf` afin de dé-commenter les directives nécessaires et ajouter celle du fichier de journalisation. Démarrez le serveur `ntp` afin de tester celui-ci. Contrôlez la présence des statistiques et le contenu du fichier `/var/log/xntpd`.

href="http://creativecommons.org/licenses/by-nc-nd/3.0/fr/">
Ce(tte) oeuvre est mise à disposition selon les termes de la Licence Creative Commons Attribution - Pas d'Utilisation Commerciale - Pas
de Modification 3.0 France. </div> </html>