Ntp - точно идут системные часики? Еще одна причина спать спокойней...

Опубликовано muff в Чт, 2009-08-20 03:12

Если вы думаете, что точность системных часов ни на что не влияет, то вы ошибаетесь. Неоднократно сталкивался, когда программы отказывались корректно работать, если часики на сервере немножко спешили или отставали. Поэтому взял за привычку в каждой сети настраивать сервер времени, а остальные машины настраивать на синхронизацию с ним.
Довольно хорошо протокол NTP описан здесь [1], поэтому отвлекаться на описание протокола не будем, а приступим сразу к настройке NTP-сервера.
В поставке FreeBSD уже идет ntp-демон, поэтому из портов ничего устанавливать не нужно, необходимо только сконфигурировать демон ntpd на синхронизацию с серверами точного времени.
Создадим конфигурационный файл демона ntpd - ntp.conf:

```
# touch /etc/ntp.conf
```

Содержание конфигурационного файла:

```
# cat /etc/ntp.conf

# Сервера, с которыми будем синхронизироваться
# iburst - ускоряем процесс синхронизации
# prefer - предпочитаемый сервер для синхронизации
server 0.ua.pool.ntp.org iburst prefer
server 1.ua.pool.ntp.org iburst
server 2.ua.pool.ntp.org iburst
server 3.ua.pool.ntp.org iburst
# driftfile - файл, в котором хранится смещение времени локальной машины относительно
# серверов точного времени
driftfile /etc/ntp/drift
# куда писать логи
logfile /var/log/ntp.log
# Отключаем мониторинг (устраняем уязвимость)
disable monitor
# список разрешенных серверов для синхронизации:
restrict 0.ua.pool.ntp.org
restrict 1.ua.pool.ntp.org
restrict 2.ua.pool.ntp.org
restrict 3.ua.pool.ntp.org
```

Ограничение на клиентов не вводим. Пусть себе синхронизируются на здоровье, те кому нужно...

Еще обращаю внимание на то, что в конфигурационном файле указываем не IP-адресс сервера синхронизации, а DNS-имя. Проверим, что за сервер отвечает при резолвинге 0.ua.pool.ntp.org:

```
# dig A 0.ua.pool.ntp.org
; <<>> DiG 9.4.3-P3 <<>> A 0.ua.pool.ntp.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42494
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
```

```
;0.ua.pool.ntp.org.          IN      A

;; ANSWER SECTION:
0.ua.pool.ntp.org.     1200    IN      A       193.34.155.4
0.ua.pool.ntp.org.     1200    IN      A       213.179.228.16
0.ua.pool.ntp.org.     1200    IN      A       91.198.10.4
0.ua.pool.ntp.org.     1200    IN      A       62.149.0.30
0.ua.pool.ntp.org.     1200    IN      A       212.111.205.110

;; Query time: 55 msec
;; SERVER: 193.227.206.51#53(193.227.206.51)
;; WHEN: Thu Aug 20 03:03:34 2009
;; MSG SIZE  rcvd: 115
```

Как видим, на это имя будут откликаться несколько хостов. Это позволяет сбалансировать нагрузку на эти сервера. Вдаваться в подробности не будем, это уже тема отдельной статьи ;)

Пора добавить в rc.conf опции для старта демона при загрузке системы:

```
# echo '#NTP' >> /etc/rc.conf
 # echo 'ntpd_enable="YES"' >> /etc/rc.conf
 # echo 'ntpd_program="/usr/sbin/ntpd"' >> /etc/rc.conf
 # echo 'ntpd_sync_on_start="YES"' >> /etc/rc.conf
```

Стартуем демон:

```
# sh /etc/rc.d/ntpd start
Starting ntpd.
```

Ждем несколько минут, необходимых для синхронизации, и проверяем состояние синхронизации:

```
 # ntpq -c peers


     remote           refid      st t when poll reach   delay   offset  jitter======
==============================================================================*garbage.vc.
ukrt 130.149.17.8     2 u  106  256  377   13.040    0.327   0.267-burka.carrier.k 2
04.123.2.72      2 u  214  256  377    0.850    2.419   0.344+shyber.tntu.edu 62.149.
0.30       2 u  184  256  377    8.309   -0.173   0.213+pechkin.vc.ukrt 193.204.114.2
33   2 u  179  256  377   13.147   -0.268   0.078
```

Попробуем разобраться, что же за вывод мы получили:

remote - имена удаленных ntp серверов;

refid - сервер, с которым производит синхронизацию удаленный сервер ntp (то есть ntp-сервер для remote);
st - стратум (вес) удаленного сервера. Чем меньше значение - тем точнее время на этом сервере;

t - тип пира (u = unicast, m = multicast);
when - указывает на то, как давно была произведена синхронизация с сервером;
poll - частота в секундах, с которой NTP демон синхронизируется с пиром;
reach - состояние доступности сервера. Это значение стабилизируется на уровне 377 если последних 8 попыток синхронизации с удаленным сервером были успешны;
delay - задержка ответа от сервера;
offset - разница в миллисекундах между системным временем и временем удаленного

сервера; значение с минусом - отставание, с плюсом - наши часики спешат;
jitter - смещение времени на удаленном сервере.

Просьба также обратить внимание на спецсимволы в поле перед remote:

"*" - указывает на сервер, с которым последний раз была произведена синхронизация;

"+" - сервер возможно использовать в качестве сервера точного времени

"-" - нервер не рекомендуется для использования.

Проверим, какой стратум у нашего сервера:

```
# ntpdate -q localhost
server 127.0.0.1, stratum 3, offset -0.000000, delay 0.02563
20 Aug 03:32:08 ntpdate[24189]: adjust time server 127.0.0.1 offset -0.000000 sec
```

В итоге у нас есть сервер точного времени, стратум которого равен 3, это позволит машинам в локальной сети синхронизироваться с даным сервером (по умолчанию стратум у ntp-клиентов равен 16).

Кстати, забыл уточнить... Синхронизация возможна только в том случае, когда стратум удаленного сервера ниже, чем локального.

Удачи и точного времени всем....

ВАЖНО! Внес изменения в конфигурационный файл **ntp.conf**, добавив опцию **disable monitor** для устранения обнаруженной уязвимости, позволяющей использовать сервер синхронизации точного времени для проведения **DDoS**-атак, путем многократного усиления трафика. В процессе атаки, запросы поражённых компьютеров, входящих в состав ботнетов, направляются не напрямую на систему жертвы, а через промежуточный усилитель трафика, путем отправки **UDP**-пакетов с подставным обратным адресом. Для усиления трафика от имени жертвы (**UDP**-пакет с подставным **IP**) на **NTP**-сервер отправляется запрос на выполнение команды **MON_GETLIST** ("**get monlist**"), результатом которого является отправка списка 600 последних IP-адресов, с которых были обращения к **NTP**-серверу. В результате размер ответа во много раз превышает исходный запрос (на загруженных серверах на запрос в 234 байт возвращается ответ в 48 КБ), что позволяет многократно усилить объём трафика, генерируемого в сторону системы жертвы. Проблему усугубляет то, что команда **monlist** выполняется без аутентификации. Проблеме подвержены все версии **ntpd** до **4.2.7p25** включительно, в выпуске **4.2.7p26** поддержка команды monlist была отключена. В качестве меры для предотвращения участия **NTP**-серверов в **DDoS**-атаках рекомендуется запретить выполнение команды мониторинга через директиву "disable monitor" или все команды выдачи статистики через опцию "**noquery**" в секции "restrict default" в **ntp.conf**. Также можно ограничить доступ к сервису **NTP** для внешних сетей или использовать модифицированные версии **ntpd**, в которых отключена поддержка команды **monlist** (достаточно пересобрать **ntpd**, удалив строку "**proto_config(PROTO_MONITOR, 0, 0., NULL);**" в файле **ntp_config.c**). Обновление с устранением уязвимости (CVE-2013-5211) уже выпущено для **FreeBSD**. Проверить наличие уязвимости в сервере можно, например, выполнив "**ntpdc -n -c monlist ip_сервера**". Если ранее использовали статью для настройки **NTP** на серверах, внесите необходимые изменения в конфигурационный файл.

Источник (получено *2025-03-14 10:50*):
http://muff.kiev.ua/content/ntp-tochno-idut-sistemnye-chasiki-eshche-odna-prichina-spat-spokoinei

Ссылки:
[1] http://www.citforum.ru/nets/semenov/4/44/ntp_4415.shtml