链滴

6- 时间同步服务、TCP_Wrappers 和 SELinux 介绍

作者：Carey

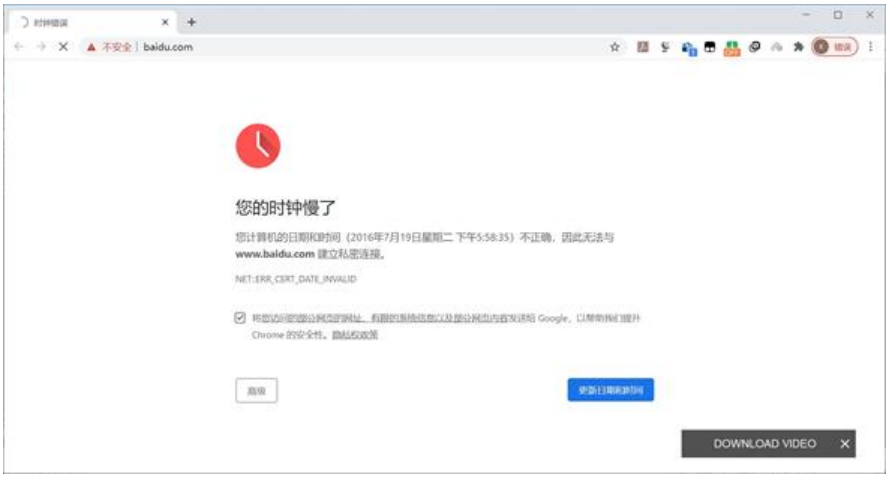
原文链接：https://ld246.com/article/1610765019861

来源网站：链滴

7 时间同步服务

加密和安全当前都离不开时间的同步，否则各种网络服务可能不能正常运行

范例: 时间错误导致证书应用出错



7.1 计时方式

7.1.1 现代计时方式

石英晶体受到电池的电力影响时，会产生规律的振动。每秒的振动次数是32768次，可以设计电路来算振动次数，当计数到32768次时，即计时1秒。1967年，瑞士人发布了世界上首款石英表

当原子从一个相对高的“能量态”迁至低的“能量态”时，会释放出电磁波，产生共振频率。依据此理， 拉比构想出了一种全新的计时仪器——原子钟（Atomic clock）

因为原子的共振频率是固定的。如：铯原子（Caesium133）的固有频率是9192631770赫兹，约合92
亿赫兹，对铯原子钟计数9192631770次，即可测量出一秒钟。很多国家（包括我国和美国NIST）
标准局，就是用铯原子钟来作为时间精度标准的。GPS系统也是用铯原子钟来计时

2008年诞生的锶（Strontium87）原子钟，固有频率为429228004229873，约合430万亿赫兹，将
度提高到了10的17次方

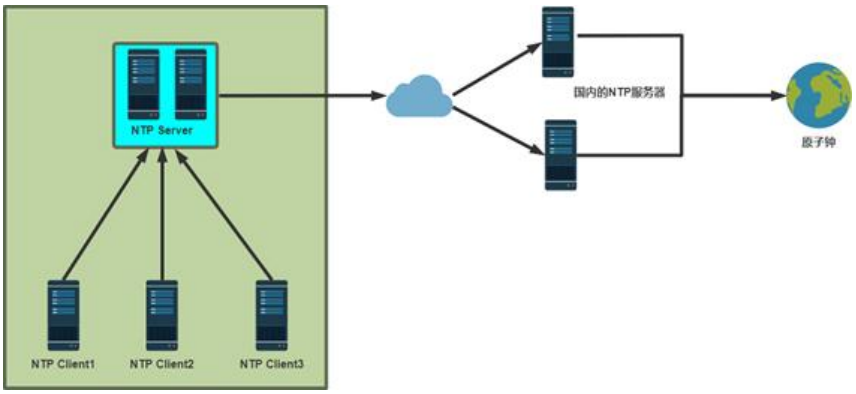
2013年镱元素（ytterbium）制成的原子钟问世，镱原子钟的固有频率约合518万亿赫兹，精度高达1
的18次方。宇宙的年龄为138亿年。如果这台镱原子钟从宇宙诞生之初就开始计时，直到今天也不会
生1秒的误差

范例：一次性的同步

```
[16:16:32 root@centos8 ~]#date -s '-1 year'
Tue Jan 14 16:16:53 CST 2020
[16:16:53 root@centos8 ~]#date
Tue Jan 14 16:17:00 CST 2020
[16:17:00 root@centos8 ~]#ping ntp.aliyun.com
PING ntp.aliyun.com (203.107.6.88) 56(84) bytes of data.
64 bytes from 203.107.6.88 (203.107.6.88): icmp_seq=1 ttl=128 time=14.8 ms
64 bytes from 203.107.6.88 (203.107.6.88): icmp_seq=2 ttl=128 time=17.3 ms
64 bytes from 203.107.6.88 (203.107.6.88): icmp_seq=3 ttl=128 time=17.2 ms
[16:19:41 root@centos8 ~]#ntpdate ntp.aliyun.com

[16:19:59 root@centos8 ~]#date
Tue Jan 14 16:20:05 CST 2020
[16:20:05 root@centos8 ~]#ntpdate time.windows.com      #这个命令在Centos8当中已经停止
用
[16:20:17 root@centos8 ~]#date
Tue Jan 14 16:20:19 CST 2020
```

7.2 时间同步服务



时间同步服务

多主机协作工作时，各个主机的时间同步很重要，时间不一致会造成很多重要应用的故障，如：加密
议，日志，集群等， 利用NTP（Network Time Protocol） 协议使网络中的各个计算机时间达到同
。目前NTP协议属于运维基础架构中必备的基本服务之一

时间同步软件实现：

- ntp

● chrony

ntp：

将系统时钟和世界协调时UTC同步，精度在局域网内可达0.1ms，在互联网上绝大多数的地方精度可达到1-50ms

项目官网：http://www.ntp.org

chrony：

实现NTP协议的的自由软件。可使系统时钟与NTP服务器，参考时钟（例如GPS接收器）以及使用手和键盘的手动输入进行同步。还可以作为NTPv4（RFC 5905）服务器和对等体运行，为网络中的计机提供时间服务。设计用于在各种条件下良好运行，包括间歇性和高度拥挤的网络连接，温度变化（算 机时钟对温度敏感），以及不能连续运行或在虚拟机上运行的系统。

通过Internet同步的两台机器之间的典型精度在几毫秒之内，在LAN上，精度通常为几十微秒。利用件时间戳或硬件参考时钟，可实现亚微秒的精度

7.3 chrony

chrony 的优势：

● 更快的同步只需要数分钟而非数小时时间，从而最大程度减少了时间和频率误差，对于并非全天24小时运行的虚拟计算机而言非常有用

● 能够更好地响应时钟频率的快速变化，对于具备不稳定时钟的虚拟机或导致时钟频率发生变化的节能技术而言非常有用

● 在初始同步后，它不会停止时钟，以防对需要系统时间保持单调的应用程序造成影响

● 在应对临时非对称延迟时（例如，在大规模下载造成链接饱和时）提供了更好的稳定性

● 无需对服务器进行定期轮询，因此具备间歇性网络连接的系统仍然可以快速同步时钟

chrony官网：https://chrony.tuxfamily.org

chrony官方文档：https://chrony.tuxfamily.org/documentation.html

7.3.1 chrony文件组成

包：chrony

两个主要程序：chronyd和chronyc

● chronyd：后台运行的守护进程，用于调整内核中运行的系统时钟和时钟服务器同步。它确定计算机增 减 时 间 的 比 率 ， 并 对 此 进 行 补 偿

● chronyc：命令行用户工具，用于监控性能并进行多样化的配置。它可以在chronyd实例控制的计机上工作，也可在一台不同的远程计算机上工作

服务unit 文件： /usr/lib/systemd/system/chronyd.service

监听端口： 服务端: 123/udp,客户端: 323/udp

配置文件： /etc/chrony.conf

7.3.2 配置文件chrony.conf

官方文档: https://chrony.tuxfamily.org/doc/3.5/chrony.conf.html

server #可用于时钟服务器，iburst 选项当服务器可达时，发送一个八个数据包而不是通常的一个数包。 包间隔通常为2秒,可加快初始同步速度
pool   #该指令的语法与server 指令的语法相似，不同之处在于它用于指定NTP服务器池而不是单个NTP服务器。池名称应解析为随时间可能会变化的多个地址
driftfile #根据实际时间计算出计算机增减时间的比率，将它记录到一个文件中，会在重启后为系统钟作出补偿
rtcsync #启用内核模式，系统时间每11分钟会拷贝到实时时钟（RTC）
allow / deny #指定一台主机、子网，或者网络以允许或拒绝访问本服务器
cmdallow / cmddeny #可以指定哪台主机可以通过chronyd使用控制命令
bindcmdaddress #允许chronyd监听哪个接口来接收由chronyc执行的命令
makestep # 通常chronyd将根据需求通过减慢或加速时钟，使得系统逐步纠正所有时间偏差。在某特定情况下，系统时钟可能会漂移过快，导致该调整过程消耗很长的时间来纠正系统时钟。该指令强chronyd在 调整期大于某个阀值时调整系统时钟
local stratum 10 #即使server指令中时间服务器不可用，也允许将本地时间作为标准时间授时给其它客户端

7.3.3 ntp客户端工具

chronyc 可以运行在交互式和非交互式两种方式，支持以下子命令

accheck   检查是否对特定主机可访问当前服务器
activity   显示有多少NTP源在线/离线
sources [-v]   显示当前时间源的同步信息
sourcestats [-v] 显示当前时间源的同步统计信息
add server   手动添加一台新的NTP服务器
clients   报告已访问本服务器的客户端列表
delete   手动移除NTP服务器或对等服务器
settime   手动设置守护进程时间
tracking   显示系统时间信息

范例：设置chronyd客户端与服务端

[09:40:54 root@centos8 ~]#vim /etc/chrony.conf
server ntp.aliyun.com iburst   #设置本台主机的ntp服务器端
allow 192.168.10.0/24   #如果要当成服务端的话需要设置这项，表示允许那个网段的主机接
local stratum 10   #服务端建议开启，表示如果本台主机的服务端断开的话是否还能给他主机提供服务
其余选项默认，如果只当服务端的话只设置server就可以了可以写域名或者IP地址
也可以写pool地址池

范例：Centos6 ntp客户端同步检查

[16:29:47 root@centos6 ~]#ntpq -p

7.3.4 公共NTP服务

● pool.ntp.org：项目是一个提供可靠易用的NTP服务的虚拟集群cn.pool.ntp.org，0- 3.cn.pool.ntp org

- 阿里云公共NTP服务器
  - Unix/linux类：ntp.aliyun.com，ntp1-7.aliyun.com
  - windows类： time.pool.aliyun.com
- 腾讯公共NTP
  - time1-5.cloud.tencent.com
- 大学ntp服务
  - s1a.time.edu.cn 北京邮电大学
  - s1b.time.edu.cn 清华大学
  - s1c.time.edu.cn 北京大学
- 国家授时中心服务器：210.72.145.44

7.3.5 时间工具

- timedatectl 时间和时区管理

```
#查看日期时间、时区及NTP状态： timedatectl

#查看时区列表：
timedatectl list-timezones

#修改时区：
timedatectl set-timezone Asia/Shanghai

#修改日期时间：
timedatectl set-time "2017-01-23 10:30:00"
#开启NTP：
timedatectl set-ntp true/false
```

- ntpdate 时间同步命令
- system-config-date：图形化配置chrony服务的工具

8 TCP Wrapper

8.1 TCP_Wrappers介绍

作者：Wieste Venema，IBM，Google，工作在第四层（传输层）的TCP协议，对有状态连接的特服务进行安全检测并实现访问控制，以库文件形式实现

某进程是否接受libwrap的控制取决于发起此进程的程序在编译时是否针对libwrap进行编译的判断服程序是否能够由tcp_wrapper进行访问控制的方法：

```
ldd  /PATH/TO/PROGRAM|grep libwrap.so
```

范例：

[10:06:45 root@centos7 ~]#ldd `which sshd` | grep libwra
libwrap.so.0 => /lib64/libwrap.so.0 (0x00007fb1bd9fa000)
[10:07:08 root@centos8 ~]#ldd `which sshd` | grep libwra
centos8已经不在使用

8.2 TCP_Wrappers的使用

配置文件：/etc/hosts.allow, /etc/hosts.deny

帮助参考：man 5 hosts_access，man 5 hosts_options

检查顺序：hosts.allow，hosts.deny（默认允许），　注意：一旦前面规则匹配，直接生效，将不继续

配置基本语法:

daemon_list@host: client_list [:options :option...]

Daemon_list@host格式

单个应用程序的二进制文件名，而非服务名，例如vsftpd
以逗号或空格分隔的应用程序文件名列表，如:sshd,vsftpd
ALL表示所有接受tcp_wrapper控制的服务程序
主机有多个IP，可用@hostIP来实现控制,如：in.telnetd@192.168.0.254

客户端Client_list格式

以逗号或空格分隔的客户端列表
基于IP地址：192.168.10.1　192.168.1.
基于主机名：www.magedu.com　.magedu.com 较少用
基于网络/掩码：192.168.0.0/255.255.255.0
基于net/prefixlen: 192.168.1.0/24（CentOS7）
基于网络组（NIS 域）：@mynetwork
内置ACL：ALL，LOCAL，KNOWN，UNKNOWN，PARANOID
EXCEPT　排除相关地址

范例：EXCEPT用法

vsftpd: 172.16. EXCEPT 172.16.100.0/24 EXCEPT 172.16.100.1

范例：只允许192.168.1.0/24的主机访问sshd

/etc/hosts.allow
sshd: 192.168.1.
/etc/hosts.deny
sshd :ALL

范例：只允许192.168.1.0/24的主机访问telnet和vsftpd服务

/etc/hosts.allow
vsftpd,in.telnetd: 192.168.1.
/etc/host.deny
vsftpd,in.telnetd: ALL

[:options]选项格式：帮助：man 5 hosts_options

- deny 主要用在/etc/hosts.allow定义“拒绝”规则，如：vsftpd: 172.16. :deny
- allow 主要用在/etc/hosts.deny定义“允许”规则，如：vsftpd:172.16. :allow
- spawn 启动一个外部程序完成执行的操作
- twist 实际动作是拒绝访问,使用指定操作替换当前服务,标准输出和ERROR发送到客户端,默认至/dev null

范例：拒绝登录

```
[10:07:18 root@centos7 ~]#vim /etc/hosts.allow
sshd:ALL:deny echo
[10:28:48 root@centos8 ~]#ssh 192.168.10.71
kex_exchange_identification: read: Connection reset by peer
```

说明：
在/etc/hosts.allow中添加，允许登录，并记录日志在/etc/hosts.deny中添加，拒绝登录，并记录日

%c 客户端信息
%s 服务器端信息
%d 服务名
%p 守护进程的PID
%% 表示%

范例：登陆时执行外部程序

```
[10:31:43 root@centos7 ~]#cat /etc/hosts.allow
sshd: ALL :spawn echo "$(date +%%F) login attempt form %c to %s,%d" >>/var/log/sshd.log
```

8.3 测试工具tcpdmatch

tcpdmatch [-d] daemon[@host] client

选项：

- -d 测试当前目录下的hosts.allow和hosts.deny

范例：

```
[10:30:21 root@centos7 ~]#vim /etc/hosts.allow
sshd: ALL :deny echo "$(date +%%F) login attempt form %c to %s,%d" >>/var/log/sshd.log
```

9 SELinux

国内基本大多数公司不使用SELinux，Centos安装之后默认会安装，ubunte没有

9.1 启用和禁用SELinux

SELinux的状态：

- enforcing：强制，每个受限的进程都必然受限
- permissive：允许，每个受限的进程违规操作不会被禁止，但会被记录于审计日志

- disabled：禁用

相关命令：

- getenforce: 获取selinux当前状态
- sestatus :查看selinux状态
- setenforce 0|1 0: 设置为permissive　1: 设置为enforcing

配置文件:

/boot/grub/grub.conf 在kernel行使用selinux=0禁用SELinux
/boot/grub2/grub.cfg 在linux16行使用selinux=0禁用SELinux
/etc/selinux/config 或 /etc/sysconfig/selinux 中 SELINUX={disabled|enforcing|permissive}