NTP and Syslog in Linux

Kevin Breit

Network Time Protocol (NTP)

Synchronizes computer time with highly accurate time services

NTP Architecture

Utilizes time server hierarchy. Each level is called a stratum.

Core servers are "Stratum 1" servers.
Servers which reference stratum 1 servers are "Stratum 2" servers.
Servers which reference stratum 2 servers are "Stratum 3" servers.
...and so on...

NTP Linux Servers

- OpenNTPd
- Generic NTP server

All configuration examples assume Ubuntu 9.04

Configuring NTP Server

/etc/ntp.conf - NTP configuration file

Main Components - Server List
server server.name.com*
server anotherserver.name.com*

Main Components - Restriction List
restrict server.name.com nomodify notrap noquery

NTP Server Selection

ntp.org maintains NTP addresses which point to volunteer NTP servers

server 0.north-america.pool.ntp.org
server 1.north-america.pool.ntp.org
server 2.north-america.pool.ntp.org
server 3.north-america.pool.ntp.org

Note: You probably don't need to use any stratum 1 and 2 servers. Move to higher stratum numbers to keep stratum 1 and 2 servers load low and in operation.

NTP Server Permissions

You only want certain servers to edit your time and only want to allow certain systems to connect to your NTP server.

restrict name.server.com nomodify notrap noquery

nomodify - Do not allow server/subnet to change ntpd settings
notrap - Do not allow server information to be sent
noquery - Do not allow server/subnet to query time

noserve - Do not serve time on this server/subnet.*

* Mostly used if server/subnet should monitor NTP server

NTP Served Subnet Permissions

Same as NTP Server Permissions, just slightly different permissions

restrict 192.168.0.0 255.255.0.0 nomodify notrap

Notice noquery is removed. This allows the 192.168.0.0/16 network to query the local NTP server

Verify NTP service

bash# ntpq -p

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+jaded.fsck.ca   128.233.150.93   2 u    1   64  377   39.131   50.669   1.504
+splenda.rustyte 173.14.47.149    2 u   19   64  377   53.863   44.622   3.131
-ns2.uplogon.com 129.6.15.28      2 u   63   64  377   47.495   63.016   3.170
*ntp.your.org    .CDMA.           1 u   61   64  377   13.221   48.200   3.377
```

These are the NTP servers the local service is polling time from. The third column is the stratum number. ntp.org assigned stratum 2 servers.

Stratum 16 servers mean it isn't synchronized properly with that specific server.

Syslog

Standard server on all Linux installs. Syslog logs local system events. Can also be used to log remote system events.

Syslog Message Levels

Syslog breaks each log message into different levels.
Note: Level 0 occurs if syslogd is down. So level 0 may happen if the system works fine

Level	Verbose	Description
0	emerg	system is unreachable
1	alert	action must be taken immediately
2	crit	the system is in a critical condition
3	err	there is an error condition
4	warning	there is a warning condition
5	notice	a normal but significant condition
6	info	purely informational message
7	debug	messages generated to debug the application

Syslog Configuration

/etc/syslog.conf

Enable network logging:
local7.debug /log/file/location.log

Network devices each send syslog messages tagged with different local numbers.

Above command would log all syslog messages tagged with local7 and debug level or higher.

Syslog Facilities

Facilities are ways to track what process a message comes from.

local0 - local7 are reserved for remote servers and network devices.

Facilities can be calculated to create a priority:

Priority = Facility * 8 + Level

Syslog Facility Numbers

0 kernel messages
1 user-level messages
2 mail system
3 system daemons
4 security/authorization messages
5 messages generated internally by syslogd
6 line printer subsystem
7 network news subsystem
8 UUCP subsystem
9 clock daemon
10 security/authorization messages
11 FTP daemon
12 NTP subsystem
13 log audit
14 log alert
15 clock daemon
16 local use 0 (local0)
17 local use 1 (local1)
18 local use 2 (local2)
19 local use 3 (local3)
20 local use 4 (local4)
21 local use 5 (local5)
22 local use 6 (local6)
23 local use 7 (local7)

Syslog Priority Example

Printer subsystem error
51 = 6 * 8 + 3

Kernel alert
1 = 0 * 8 + 1

Syslog Verification

View output file configured in syslog.conf

Q&A