Wednesday, June 15, 2022 9:15 PM

NTP Authentication: Server Side

the tool ntp-keygen -M in order to "**Generate a new symmetric keys** file containing 10 MD5 keys, and if OpenSSL is available, 10 SHA keys". I'm doing it in the /etc/ folder to have the key file in the correct place. Note that ntp-keygen in fact generates a keyfile as well as a link called "ntpjkey_md5_localhost.localhost". Finally, I am showing the keys here:

```
[root@localhost ~]# ls /etc/ntp/
crypto  keys  ntpkey_MD5key_localhost.localdomain.3864274003  ntpkey_md5_localhost.localdomain  step-tickers
[root@localhost ~]#
```

```
# ntpkey_MD5key_localhost.localdomain.3864274003
# Wed Jun 15 15:11:43 2022

 1 MD5 OqW4GIjiDVlq<udlFcLw  # MD5 key
 2 MD5 rADO+&szR~~eT7k[0GIF  # MD5 key
 3 MD5 +q[TnkR6Og:5U2,O1/[2  # MD5 key
 4 MD5 QDaTmi"\$G}cDM'N`&!,  # MD5 key
 5 MD5 O}[,B"&c@jJu$g9RG]vy  # MD5 key
 6 MD5 ]Ts>*;vP5^(TfrA-ul0_  # MD5 key
 7 MD5 {<zyN;Z-T~9TKe'dNA;y  # MD5 key
 8 MD5 {jnR`8?v4uN8MA3R~[8!  # MD5 key
 9 MD5 iS*I;iH5$rrf2'.c2XJu  # MD5 key
10 MD5 GXt8Y'A%JRd^cHEX}MTK  # MD5 key
11 SHA1 40450c20a081a066310a33f0fdea0e7250a7c6c6  # SHA1 key
12 SHA1 f0f431dcac79664f8b94ba3fefd6c8941c2a07da  # SHA1 key
13 SHA1 7edde6b7a17af584be1660e8d99b3461397c872a  # SHA1 key
14 SHA1 a2f79989473a60d4f3aecd0b546cab17c80e2bc4  # SHA1 key
15 SHA1 fc0f9e70165bb42ab416718b6f8b14784cb7da0f  # SHA1 key
16 SHA1 4d92ec50319f845be6647774bc92fd72dea94009  # SHA1 key
17 SHA1 b8b350b440f32ecad04abb8fd322799641c4f724  # SHA1 key
18 SHA1 e7618e0a9aded405c12754506c3e84f8fce7fcbc  # SHA1 key
19 SHA1 ee538f497bbdd2490afef781f586e6d90100aa68  # SHA1 key
20 SHA1 987fc879a6464f70082d57f229a21caf6f7c4f66  # SHA1 key
```

Edit the following code in /etc/ntp.conf file

```
# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/ntpkey_md5_localhost.localdomain

# Specify the key identifiers which are trusted.
trustedkey 11
```

After editing the conf file, restart the ntpd service.

Wednesday, June 15, 2022 9:29 PM

NTP Client Setup

Note that when you're using multiple NTP servers (which I highly recommend, refer to Why should I run own NTP Servers?) you must use different keys/IDs for each of them. Obviously you can't use the same "key number 11" for different NTP servers as far as they're using different randomly generated keys. In my lab I'm using three stratum 1 NTP servers (Pi DCF77, Pi GPS, Meinberg M200) with the key IDs 11, 12, and 13.

Everything takes place solely on the NTP client. The first step is to create the ntp.keys file with the needed keys. **sudo vim/etc/ntp.keys** In my case it's:

```
11 SHA1 40450c20a081a066310a33f0fdea0e7250a7c6c6  # SHA1 key
~
~
~
~
~
~
~
~
```

The second step is to refer to this ntp.keys file, trusting those three keys, and using them on the appropriate NTP servers. sudo nano /etc/ntp.conf, adding/modifying those lines:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 192.168.29.128 key 11
#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

# 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/ntp.keys

# Specify the key identifiers which are trusted.
trustedkey 11
```

At last **restart ntpd service**.