Instructions for using the NIST authenticated Network Time Protocol (NTP) server

These instructions explain how to add symmetric-key authentication to the most common version of the NTP software. Users with special requirements or who are using a non-standard version of NTP should contact NIST for assistance. We will try to provide as much assistance as possible. Users who wish to add authentication to the NTP process of a network appliance (such as a gateway, firewall or router) should contact the supplier to verify that the embedded NTP algorithm supports the symmetric key encryption algorithm.

The NIST authenticated NTP server

The authenticated version of NTP will be supported by the NIST time servers listed as authenticated NTP servers here: http://tf.nist.gov/tf-cgi/servers.cgi

The same key can be used in a request to any NIST authenticated server.

Requesting a key

To request a key, the user should send a letter to NIST using the US mail or a FAX machine (e-mail is not acceptable). The request should contain the following information:

1. Name and postal street address of the organization or individual.
2. Name and contact information for the system operator and an alternate contact if possible. These should include the e-mail addresses and the preferred contact method.
3. Network IP address of the client system that will be used to query the NIST server. A network name is desirable but not required, since the system will authenticate the request using IP addresses only. Users may request up to 4 contiguous IP addresses that will share the same key.

This information should be sent to:

National Institute of Standards and Technology
Network Time Service - Mail stop 847
325 Broadway St.
Boulder, Colorado 80305
FAX: 303 497 6461

The reply from NIST will contain a key number, which is a decimal integer, and a key value, which is a string of printing characters. In the following instructions, the user should replace the parameters <key number> and <key value> with the actual values received from NIST. The key is in MD5 format by default. Users may explicitly request a key in SHA-1 format.

The key file

The user must add the key number and the key value to a key file. The file can have any name and be located in any directory, but is usually named ntp.keys and is usually located in the same directory as the NTP software and configuration file. The values received from NIST are added to the key file using a single line of text:

<key number> M <key value>

The letter M specifies that the key is in MD5 format. For example:

```
12345 M BlahBlahBlah
```

If the user requests a key in SHA-1 format, the "M" should be replaced by "SHA1".
[Note that this identifier may be different on some systems.]

The key value must be entered in upper and lower case exactly as received from NIST. The key file should be owned by root and should not be readable by normal users. (See exception below) Each user can request a key in MD5 format or SHA-1 format, but not both.

Testing the key

After the key has been entered into the key file, it can be tested using the utility program `ntpdate`. For example, suppose that the key received from NIST was number 12345 and that the key number and the corresponding value have been added to the key file as described above. The following command will use this key to contact the NIST server and report the results of the conversation. The switches have the following meanings:

-d Run in debug mode: print intermediate results and do not adjust the clock -a The following integer specifies the key number -k The following string specifies the name of the key file

The IP address specifies the address of the server to be queried. The example uses 1.2.3.4 for the IP address of the NIST time server. This should be replaced with the IP address of one of the NIST servers that supports authentication, as listed here: http://tf.nist.gov/tf-cgi/servers.cgi

The command:

```
Test1> ntpdate -d -a 12345 -k /local/bin/ntp.keys 1.2.3.4
```

The reply:

```
30 Apr 08:51:49 ntpdate[3269]: ntpdate version=3.5f; Mon Oct 28
17:10:52 MST 1996 (1)
transmit(1.2.3.4)
receive(1.2.3.4)
receive: authentication passed
transmit(1.2.3.4)
receive(1.2.3.4)
receive: authentication passed
transmit(1.2.3.4)
receive(1.2.3.4)
receive: authentication passed
transmit(1.2.3.4)
receive(1.2.3.4)
receive: authentication passed
transmit(1.2.3.4)
server 1.2.3.4, port 123
stratum 1, precision -31, leap 00, trust 000
refid [NIST], delay 0.03233, dispersion 0.00124
transmitted 4, in filter 4
reference time: c9e08103.7739c630 Mon, Apr 30 2007 8:51:47.465
originate timestamp: c9e08105.8e384cc1 Mon, Apr 30 2007 8:51:49.555

transmit timestamp: c9e08105.8e1d5000 Mon, Apr 30 2007 8:51:49.555
filter delay: 0.03233 0.03238 0.03249 0.03244
              0.00000 0.00000 0.00000 0.00000
filter offset: -0.00156 -0.00296 -0.00304 -0.00301
               0.000000 0.000000 0.000000 0.000000
delay 0.03233, dispersion 0.00124offset -0.001566

30 Apr 08:51:49 ntpdate[3269]: adjust time server 1.2.3.4 offset-
0.001566 sec
```

If the key number or key value are not correct then the message *"authentication passed"* will be replaced with *"authentication failed."* If the response shows `transmit` messages with no corresponding *receive* responses then either the IP address was not registered with NIST or a firewall or network router is blocking the connection to the time server.

Note: When *ntpdate* is run in debug mode (as in the example above), it is normally not a privileged program and can be run by any user. The user must have read access to the key file in this case.

Configuring the daemon process NTPD

In order to use authentication, the following commands must be added to the ntp configuration file (usually named ntp.conf). These changes should be made after the key has been added to the key file as described above. The symbol "#" introduces a comment, which continues for the remainder of the line. The NTP daemon process must be restarted after the file has been edited.

```
#
#     authentication is normally enabled by default
#
enable auth
#
#     define the name of the key file
#
keys     /local/bin/ntp.keys
#
#     specify the key(s) that can be trusted
#     replace <key number> with the key number
#     received from NIST
#
#     For example: trustedkey 12345
#
trustedkey <key number>
#
#     specify the address of the server and the
#     key number to be used when processing a query
#     the server can be specified using its name or
#     its IP address.
#     the value 12345 should be replaced with the
#     actual key number received from NIST
#     and the address 1.2.3.4 should be replaced
#     with the address of a NIST authenticated time
#     server.

server 1.2.3.4 key 12345
```

It is helpful to monitor the performance of the NTP daemon to confirm that the authentication algorithm is working as expected. The NTP daemon provides a number of monitoring tools that can be used for this purpose. For example, the peerstats command will provide information on the status of the connections to the servers that are being used to synchronize the system time. To enable this report, the following commands would be added to the NTP configuration file:

```
#
#     enable monitoring and reporting of statistics
```

```
#
enable monitor
enable stats
#
#     turn on reporting of the peer statistics
#
statistics peerstats
#
#     the file for the report will be named peerstats with
#     the date appended. The full name of the file
#     will be peerstats.yyyymmdd.
#     a new file will be created every day at 0 hours UTC.
#
filegen peerstats file peerstats type day
#
#     the following command specifies the full name of
#     the directory where the files will be located
#
statsdir /local/bin/
```

The daemon process will add an entry into the peerstats file each time the client queries a server. The entry will be in the following form:

54237 86332.222 1.2.3.4 f624 -0.011106682 0.000251015 0.000953898 0.000073756

The first two parameters give the time of the query as the MJD (Modified Julian Day number) and the UTC second of the day. The third parameter gives the IP address of the remote system. The fourth parameter describes the state of the query using the hexadecimal representation of a series of bits. The significance of each bit is described in Appendix B of RFC1305. Using the convention that the most significant bit of the state is bit 0, the first hexadecimal digit of the state should be “f” to indicate that:

Bit 0: peer is configured
Bit 1: authentication is enabled
Bit 2: authentication is ok
Bit 3: peer is reachable

If authentication is not used, then bits 1 and 2 will be 0, and the first digit will be 9 instead of f. The “6” in the second digit signals that this server is being used to synchronize the local clock. If the client is querying more than one server, then the one that is selected to synchronize the clock will have a 6 as the second digit and the other status words will normally have a 4 in that position.

The remaining parameters describe the offset, delay, dispersion, and jitter of the query.
These parameters are in units of seconds and are described in RFC1305.

The NTP documentation describes other reports that can be generated by the daemon process. We recommend that some monitoring and reporting process be used to verify the proper operation of the daemon.

Comments or questions should be sent to: jlevine@boulder.nist.gov