NAME

ntp.conf - NTP server configuration file

SYNOPSIS

ntp.conf

DESCRIPTION

Ordinarily, **ntpd** reads the *ntp.conf* configuration file at startup time in order to determine the synchronization sources and operating modes. It is also possible to specify a working, although limited, configuration entirely on the command line, obviating the need for a configuration file. This may be particularly useful when the local host is to be configured as a broadcast/multicast client, with all peers being determined by listening to broadcasts at run time.

Usually, the configuration file is installed in the */etc* directory, but could be installed elsewhere (see the -c *conffile* command line option). The file format is similar to other Unix configuration files - comments begin with a # character and extend to the end of the line; blank lines are ignored.

Configuration commands consist of an initial keyword followed by a list of arguments, some of which may be optional, separated by whitespace. Commands may not be continued over multiple lines. Arguments may be host names, host addresses written in numeric, dotted-quad form, integers, floating point numbers (when specifying times in seconds) and text strings. Optional arguments are delimited by [ ] in the following descriptions, while alternatives are separated by |. The notation [...] means an optional, indefinite repetition of the last item before the [...].

Following is a description of the configuration commands in NTPv4. There are two classes of commands, configuration commands that configure an association with a remote server, peer or reference clock, and auxiliary commands that specify environmental variables that control various related operations.

Configuration Commands

The various modes are determined by the command keyword and the required IP address. Addresses are classed by type as (s) a remote server or peer (IPv4 class A, B and C), (b) the broadcast address of a local interface, (m) a multicast address (IPv4 class D), or (r) a reference clock address (127.127.x.x). The options that can be used with these commands are listed below.

If the Basic Socket Interface Extensions for IPv6 (RFC-2553) is detected, support for the IPv6 address family is generated in addition to the default support of the IPv4 address family. IPv6 addresses can be identified by the presence of colons : in the address field. IPv6 addresses can be used almost everywhere where IPv4 addresses can be used, with the exception of reference clock addresses, which are always IPv4. Note that in contexts where a host name is expected, a -4 qualifier preceding the host name forces DNS resolution to the IPv4 namespace, while a -6 qualifier forces DNS resolution to the IPv6 namespace.

There are three types of associations: persistent, preemptable and ephemeral. Persistent associations are mobilized by a configuration command and never demobilized. Preemptable associations, which are new to NTPv4, are mobilized by a configuration command which includes the **prempt** flag and are demobilized by timeout or error. Ephemeral associations are mobilized upon arrival of designated messages and demobilized by timeout or error.

server *address* [*options* ...]

peer *address* [*options* ...]

broadcast *address* [*options* ...]

manycastclient *address* [*options* ...]

These four commands specify the time server name or address to be used and the mode in which to operate. The *address* can be either a DNS name or a IP address in dotted-quad notation. Additional information on association behavior can be found in the Association Management page.

server For type s and r addresses (only), this command normally mobilizes a persistent client mode association with the specified remote server or local reference clock. If the preempt flag is specified, a preemptable association is mobilized instead. In client mode the client clock can synchronize to the remote server or local reference clock, but the remote server can never be synchronized to the client clock. This command should NOT be used for type b or m addresses.

peer For type s addresses (only), this command mobilizes a persistent symmetric-active mode association with the specified remote peer. In this mode the local clock can be synchronized to the remote peer or the remote peer can be synchronized to the local clock. This is useful in a network of servers where, depending on various failure scenarios, either the local or remote peer may be the better source of time. This command should NOT be used for type b, m or r addresses.

broadcast

For type b and m addresses (only), this command mobilizes a persistent broadcast mode association. Multiple commands can be used to specify multiple local broadcast interfaces (subnets) and/or multiple multicast groups. Note that local broadcast messages go only to the interface associated with the subnet specified, but multicast messages go to all interfaces.

In broadcast mode the local server sends periodic broadcast messages to a client population at the *address* specified, which is usually the broadcast address on (one of) the local network(s) or a multicast address assigned to NTP. The IANA has assigned the multicast group address IPv4 224.0.1.1 and IPv6 ff05::101 (site local) exclusively to NTP, but other nonconflicting addresses can be used to contain the messages within administrative boundaries. Ordinarily, this specification applies only to the local server operating as a sender; for operation as a broadcast client, see the **broadcastclient** or **multicastclient** commands below.

manycastclient

For type m addresses (only), this command mobilizes a preemptable manycast client mode association for the multicast group address specified. In this mode a specific address must be supplied which matches the address used on the manycastserver command for the designated manycast servers. The NTP multicast address 224.0.1.1 assigned by the IANA should NOT be used, unless specific means are taken to avoid spraying large areas of the Internet with these messages and causing a possibly massive implosion of replies at the sender.

The **manycastclient** command specifies that the host is to operate in client mode with the remote servers that are discovered as the result of broadcast/multicast messages. The client broadcasts a request message to the group address associated with the specified *address* and specifically enabled servers respond to these messages. The client selects the servers providing the best time and continues as with the server command. The remaining servers are discarded as if never heard.

Command Options

autokey

All packets sent to and received from the server or peer are to include authentication fields encrypted using the autokey scheme described in the Authentication Options page. This option is valid with all commands.

burst When the server is reachable, send a burst of eight packets instead of the usual one. The packet spacing is normally 2 s; however, the spacing between the first and second packets can be changed with the **calldelay** command to allow additional time for a modem or ISDN call to complete. This option is valid with only the **server** command and is a recommended option with this command when the **maxpoll** option is 11 or greater.

iburst When the server is unreachable, send a burst of eight packets instead of the usual one. The packet spacing is normally 2 s; however, the spacing between the first and second packets can be changed with the **calldelay** command to allow additional time for a modem or ISDN call to complete. This option is valid with only the **server** command and is a recommended option with this command.

key *key*
All packets sent to and received from the server or peer are to include authentication fields encrypted using the specified key identifier with values from 1 to 65534, inclusive. The default is to include no encryption field. This option is valid with all commands.

minpoll *minpoll*, **maxpoll** *maxpoll*
These options specify the minimum and maximum poll intervals for NTP messages, in seconds as a power of two. The maximum poll interval defaults to 10 (1,024 s), but can be increased by the maxpoll option to an upper limit of 17 (36.4 h). The minimum poll interval defaults to 6 (64 s), but can be decreased by the minpoll option to a lower limit of 4 (16 s). These option are valid only with the **server** and **peer** commands.

mode *option*
Pass the *option* to a reference clock driver, where *option* is an integer in the range from 0 to 255, inclusive. This option is valid only with type r addresses.

noselect
Marks the server as unused, except for display purposes. The server is discarded by the selection algorithm. This option is valid only with the **server** and **peer** commands.

preempt
Specifies the association as preemptable rather than the default persistent. This option is valied only with the **server** command.

prefer Marks the server as preferred. All other things being equal, this host will be chosen for synchronization among a set of correctly operating hosts. See the Mitigation Rules and the **prefer** Keyword page for further information. This option is valid only with the **server** and **peer** commands.

true Force the association to assume truechimer status; that is, always survive the selection and clustering algorithms. This option can be used with any association, but is most useful for reference clocks with large jitter on the serial port and precision pulse-per-second (PPS) signals. Caution: this option defeats the algorithms designed to cast out falsetickers and can allow these sources to set the system clock. This option is valid only with the **server** and **peer** commands.

ttl *ttl* This option is used only with broadcast server and manycast client modes. It specifies the time-to-live *ttl* to use on broadcast server and multicast server and the maximum *ttl* for the expanding ring search with manycast client packets. Selection of the proper value, which defaults to 127, is something of a black art and should be coordinated with the network administrator.

version *version*
Specifies the version number to be used for outgoing NTP packets. Versions 1-4 are the choices, with version 4 the default. This option is valid only with the **server**, **peer** and **broadcast** commands.

xleave Operate in interleaved mode (symmetric and broadcast modes only). (see NTP Interleaved Modes)

Auxiliary Commands

broadcastclient [**novolley**]
This command enables reception of broadcast server messages to any local interface (type b) address. Ordinarily, upon receiving a message for the first time, the broadcast client measures the nominal server propagation delay using a brief client/server exchange with

the server, after which it continues in listen-only mode. If the **novolley** keyword is present, the exchange is not used and the value specified in the **broadcastdelay** command is used or, if the **broadcastdelay** command is not used, the default 4.0 ms. Note that, in order to avoid accidental or malicious disruption in this mode, both the server and client should operate using symmetric key or public key authentication as described in the Authentication Options page. Note that the **novolley** keyword is incompatible with public key authentication.

manycastserver *address* [...]
This command enables reception of manycast client messages to the multicast group address(es) (type m) specified. At least one address is required. The NTP multicast address 224.0.1.1 assigned by the IANA should NOT be used, unless specific means are taken to limit the span of the reply and avoid a possibly massive implosion at the original sender. Note that, in order to avoid accidental or malicious disruption in this mode, both the server and client should operate using symmetric key or public key authentication as described in the Authentication Options page.

multicastclient *address* [...]
This command enables reception of multicast server messages to the multicast group address(es) (type m) specified. Upon receiving a message for the first time, the multicast client measures the nominal server propagation delay using a brief client/server exchange with the server, then enters the broadcast client mode, in which it synchronizes to succeeding multicast messages. Note that, in order to avoid accidental or malicious disruption in this mode, both the server and client should operate using symmetric key or public key authentication as described in the Authentication Options page.

Authentication Commands

autokey [*logsec*]
Specifies the interval between regenerations of the session key list used with the autokey feature. Note that the size of the key list for each association depends on this interval and the current poll interval. The default value is 12 (4096 s or about 1.1 hours). For poll intervals above the specified interval, a session key list with a single entry will be regenerated for every message sent.

revoke [*logsec*]
Specifies the interval between recomputations of the private value used with the autokey feature, which ordinarily requires an expensive public- key computation. The default value is 12 (65,536 s or about 18 hours). For poll intervals above the specified interval, a new private value will be recomputed for every message sent.

Miscellaneous Options

driftfile *driftfile*
This command specifies the name of the file use to record the frequency offset of the local clock oscillator. If the file exists, it is read at startup in order to set the initial frequency offset and then updated once per hour with the current frequency offset computed by the daemon. If the file does not exist or this command is not given, the initial frequency offset is assumed to be zero. In this case, it may take some hours for the frequency to stabilize and the residual timing errors to subside.

The file format consists of a single line containing a single floating point number, which records the frequency offset measured in parts-per-million (PPM). The file is updated by first writing the current drift value into a temporary file and then renaming this file to replace the old version. This implies that ntpd must have write permission for the directory the drift file is located in, and that file system links, symbolic or otherwise, should be avoided.

enable [auth | bclient | calibrate | kernel | monitor | ntp | pps | stats]

disable [auth | bclient | calibrate | kernel | monitor | ntp | pps | stats]
Provides a way to enable or disable various server options. Flags not mentioned are unaffected. Note that all of these flags can be controlled remotely using the **ntpdc** utility program.

auth Enables the server to synchronize with unconfigured peers only if the peer has been correctly authenticated using either public key or private key cryptography. The default for this flag is enable.

bclient
Enables the server to listen for a message from a broadcast or multicast server, as in the **multicastclient** command with default address. The default for this flag is disable.

calibrate
Enables the calibrate feature for reference clocks. The default for this flag is disable.

kernel Enables the kernel time discipline, if available. The default for this flag is enable if support is available, otherwise disable.

monitor
Enables the monitoring facility. See the **ntpdc** program and the **monlist** command or further information. The default for this flag is enable.

ntp Enables time and frequency discipline. In effect, this switch opens and closes the feedback loop, which is useful for testing. The default for this flag is enable.

pps Enables the pulse-per-second (PPS) signal when frequency and time is disciplined by the precision time kernel modifications. See the A Kernel Model for Precision Timekeeping page for further information. The default for this flag is disable.

stats Enables the statistics facility. See the Monitoring Options page for further information. The default for this flag is disable.

includefile *includefile*
This command allows additional configuration commands to be included from a separate file. Include files may be nested to a depth of five; upon reaching the end of any include file, command processing resumes in the previous configuration file. This option is useful for sites that run **ntpd** on multiple hosts, with (mostly) common options (e.g., a restriction list).

interface [**listen | ignore | drop**] [**all | ipv4 | ipv6 | wildcard |** *name* **|** *address*[*/prefixlen*]]
This command controls which network addresses **ntpd** opens, and whether input is dropped without processing. The first parameter determines the action for addresses which match the second parameter. That parameter specifies a class of addresses, or a specific interface name, or an address. In the address case, *prefixlen* determines how many bits must match for this rule to apply. **ignore** prevents opening matching addresses, **drop** causes **ntpd** to open the address and drop all received packets without examination. Multiple **interface** commands can be used. The last rule which matches a particular address determines the action for it. **interface** commands are disabled if any **-I**, **--interface**, **-L**, or **--novirtualips** command-line options are used. If none of those options are used and no **interface** actions are specified in the configuration file, all available network addresses are opened. The **nic** command is an alias for **interface**.

FILES

/etc/ntp.conf

NOTES

Note that this manual page shows only the most important configuration commands. The full documentation (see below) contains more details.

BUGS

The syntax checking is not picky; some combinations of ridiculous and even hilarious options and modes may not be detected.

SEE ALSO

ntpd(8)

The complete documentation can be found at */usr/share/doc/ntp-doc/html/ntpd.html#cfg* in the package ntp-doc.