NAME

ntp_acc - Access Control Options

ACCESS CONTROL SUPPORT

The **ntpd** daemon implements a general purpose access control list (ACL) containing address/match entries sorted first by increasing address values and then by increasing mask values. A match occurs when the bitwise AND of the mask and the packet source address is equal to the bitwise AND of the mask and address in the list. The list is searched in order with the last match found defining the restriction flags associated with the entry.

An example may clarify how it works. Our campus has two class-B networks, 128.4 for the ECE and CIS departments and 128.175 for the rest of campus. Let's assume (not true!) that subnet 128.4.1 homes critical services like class rosters and spread sheets. A suitable ACL might be

```
restrict default nopeer                                    # deny new associations
restrict 128.175.0.0 mask 255.255.0.0                  # allow campus access
restrict 128.4.0.0 mask 255.255.0.0 none     # allow ECE and CIS access
restrict 128.4.1.0 mask 255.255.255.0 notrust # require authentication on subnet 1
restrict time.nist.gov                                     # allow access
```

While this facility may be useful for keeping unwanted, broken or malicious clients from congesting innocent servers, it should not be considered an alternative to the NTP authentication facilities. Source address based restrictions are easily circumvented by a determined cracker.

ACCESS CONTROL COMMANDS

discard [average *avg* **][minimum** *min* **] [monitor** *prob* **]**

Set the parameters of the rate control facility which protects the server from client abuse. If the **limited** flag is present in the ACL, packets that violate these limits are discarded. If in addition the **kod** restriction is present, a kiss-o'-death packet is returned.

average *avg*

Specify the minimum average interpacket spacing (minimum average headway time) in log2 s with default 3.

minimum *min*

Specify the minimum interpacket spacing (guard time) in log2 s with default 1.

monitor Specify the probability of discard for packets that overflow the rate-control window. This is a performance optimization for servers with aggregate arrivals of 1000 packets per second or more.

restrict *address* **[mask** *mask***] [***flag***][...]**

The *address* argument expressed in dotted-quad form is the address of a host or network. Alternatively, the *address* argument can be a valid host DNS name, but it must be resolvable at the time when **ntpd** is started and if it's resolved to multiple addresses, only the first address will be added to the list. The *mask* argument expressed in dotted-quad form defaults to 255.255.255.255, meaning that the *address* is treated as the address of an individual host. A default entry (address 0.0.0.0, mask 0.0.0.0) is always included and is always the first entry in the list. Note that the text string **default**, with no mask option, may be used to indicate the default entry. Some flags have the effect to deny service, some have the effect to enable service and some are conditioned by other flags. The flags. are not orthogonal, in that more restrictive flags will often make less restrictive ones redundant. The flags that deny service are classed in two categories, those that restrict time service and those that restrict informational queries and attempts to do run-time reconfiguration of the server. One or more of the following flags may be specified:

flake Discard received NTP packets with probability 0.1; that is, on average drop one packet in ten. This is for testing and amusement. The name comes from Bob Braden's *flakeway*, which once did a similar thing for early Internet testing.

ignore Deny packets of all kinds, including **ntpq** and **ntpdc** queries.

kod Send a kiss-o'-death (KoD) packet if the **limited** flag is present and a packet violates the rate limits established by the **discard** command. KoD packets are themselves rate limited for each source address separately. If this flag is not present, packets that violate the rate limits are discarded.

limited Deny time service if the packet violates the rate limits established by the **discard** command. This does not apply to **ntpq** and **ntpdc** queries.

lowpriotrap
Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first served basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps.

mssntp Enable Microsoft Windows MS-SNTP authentication using Active Directory services. Note: Potential users should be aware that these services involve a TCP connection to another process that could potentially block, denying services to other users. Therefore, this flag should be used only for a dedicated server with no clients other than MS-SNTP.

nomodify
Deny **ntpq** and **ntpdc** queries which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.

noquery
Deny **ntpq** and **ntpdc** queries. Time service is not affected.

nopeer Deny packets that might mobilize an association unless authenticated. This includes broadcast, symmetric-active and manycast server packets when a configured association does not exist. Note that this flag does not apply to packets that do not attempt to mobilize an association.

noserve Deny all packets except **ntpq** and **ntpdc** queries.

notrap Decline to provide mode 6 control message trap service to matching hosts. The trap service is a subsystem of the **ntpdc** control message protocol which is intended for use by remote event logging programs.

notrust Deny packets that are not cryptographically authenticated. Note carefully how this flag interacts with the **auth** option of the **enable** and **disable** commands. If **auth** is enabled, which is the default, authentication is required for all packets that might mobilize an association. If **auth** is disabled, but the **notrust** flag is not present, an association can be mobilized whether or not authenticated. If **auth** is disabled, but the **notrust** flag is present, authentication is required only for the specified address/mask range.

ntpport

non-ntpport
This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). Both **ntpport** and **non-ntpport** may be specified. The **ntpport** is considered more specific and is sorted later in the list.

version Deny packets that do not match the current NTP version.

Default restriction list entries with the flags **ignore, ntpport**, for each of the local host's interface addresses

are inserted into the table at startup to prevent the server from attempting to synchronize to its own time. A default entry is also always present, though if it is otherwise unconfigured; no flags are associated with the default entry (i.e., everything besides your own NTP server is unrestricted).

SEE ALSO

ntp.conf(5)

The official HTML documentation.

This file was automatically generated from HTML source.