NAME

audispd.conf − the audit event dispatcher configuration file

DESCRIPTION

audispd.conf is the file that controls the configuration of the audit event dispatcher. Each line should contain one configuration keyword, an equal sign, and then followed by appropriate configuration information. All option names and values are case insensitive. The keywords recognized are listed and described below. Each line should be limited to 160 characters or the line will be skipped. You may add comments to the file by starting the line with a '#' character.

q_depth
This is a numeric value that tells how big to make the internal queue of the audit event dispatcher. A bigger queue lets it handle a flood of events better, but could hold events that are not processed when the daemon is terminated. If you get messages in syslog about events getting dropped, increase this value. The default value is 80.

overflow_action
This option determines how the daemon should react to overflowing its internal queue. When this happens, it means that more events are being received than it can get rid of. This error means that it is going to lose the current event its trying to dispatch. It has the following choices: *ignore*, *syslog*, *suspend*, *single*, and *halt*. If set to *ignore*, the audisp daemon does nothing. *syslog* means that it will issue a warning to syslog. *suspend* will cause the audisp daemon to stop processing events. The daemon will still be alive. The *single* option will cause the audisp daemon to put the computer system in single user mode. *halt* option will cause the audisp daemon to shutdown the computer system.

priority_boost
This is a non-negative number that tells the audit event dispatcher how much of a priority boost it should take. This boost is in addition to the boost provided from the audit daemon. The default is 4. No change is 0.

max_restarts
This is a non-negative number that tells the audit event dispatcher how many times it can try to restart a crashed plugin. The default is 10.

name_format
This option controls how computer node names are inserted into the audit event stream. It has the following choices: *none*, *hostname*, *fqd*, *numeric*, and *user*. *None* means that no computer name is inserted into the audit event. *hostname* is the name returned by the gethostname syscall. The *fqd* means that it takes the hostname and resolves it with dns for a fully qualified domain name of that machine. *Numeric* is similar to fqd except it resolves the IP address of the machine. *User* is an admin defined string from the name option. The default value is *none*.

name This is the admin defined string that identifies the machine if user is given as the name_format option.

SEE ALSO

audispd(8)