NAME

ausearch_add_timestamp_item_ex − build up search rule

SYNOPSIS

#include <auparse.h>

int ausearch_add_timestamp_item_ex(auparse_state_t *****au*,const***char***"*** *op*,**time_t"***sec*,**unsigned"***milli*,**unsigned"***serial*,**ausearch_rule_t"***how);"*

DESCRIPTION

ausearch_add_timestamp_item adds an event time condition to the current audit search expression. The search conditions can then be used to scan logs, files, or buffers for something of interest. The op parameter specifies the desired comparison. Legal op values are <, <=, >=, > and =. The left operand of the comparison operator is the timestamp of the examined event, the right operand is specified by the sec, milli, and serial parameters.

The how value determines how this search condition will affect the existing search expression if one is already defined. The possible values are:

AUSEARCH_RULE_CLEAR
Clear the current search expression, if any, and use only this search condition.

AUSEARCH_RULE_OR
If a search expression *E* is already configured, replace it by **(***E* **||** *this_search_condition***)**.

AUSEARCH_RULE_AND
If a search expression *E* is already configured, replace it by **(***E* **&&** *this_search_condition***)**.

RETURN VALUE

Returns −1 if an error occurs; otherwise, 0 for success.

APPLICATION USAGE

Use **ausearch_add_item**(3) and **ausearch_add_interpreted_item**(3) to add conditions that check audit record fields. Use **ausearch_add_expression**(3) to add complex search expressions using a single function call.

SEE ALSO

ausearch_add_expression(3), **ausearch_add_item**(3), **ausearch_add_interpreted_item**(3), **ausearch_add_regex**(3), **ausearch_set_stop**(3), **ausearch_clear**(3), **ausearch_next_event**(3), **ausearch_cur_event**(3), **ausearch−expression**(5).

AUTHOR

Miloslav Trmac