

NAME

`ausearch_add_expression` – build up search expression

SYNOPSIS

```
#include <auparse.h>
```

```
int ausearch_add_expression(auparse_state_t *au, const char *expression, char **error, ausearch_rule_t how);"
```

DESCRIPTION

ausearch_add_item adds an expression to the current audit search expression. The search conditions can then be used to scan logs, files, or buffers for something of interest. The *expression* parameter contains an expression, as specified in **ausearch-expression(5)**. The *how* parameter determines how this search expression 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 expression.

AUSEARCH_RULE_OR

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

AUSEARCH_RULE_AND

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

The caller must free the error message using **free(3)**. If an error message is not available or can not be allocated, **error* is set to **NULL**.

SEE ALSO

ausearch_add_item(3), **ausearch_add_interpreted_item(3)**, **ausearch_add_timestamp_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