

NAME

auparse_normalize_get_event_kind, auparse_normalize_subject_kind, auparse_normalize_get_action, auparse_normalize_obj

SYNOPSIS

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

Metadata Functions:

```
const char *auparse_normalize_get_event_kind(const auparse_state_t *au);
const char *auparse_normalize_subject_kind(const auparse_state_t *au);
const char *auparse_normalize_get_action(const auparse_state_t *au);
const char *auparse_normalize_object_kind(const auparse_state_t *au);
const char *auparse_normalize_how(const auparse_state_t *au);
```

Positioning Functions:

```
int auparse_normalize_session(auparse_state_t *au);
int auparse_normalize_subject_primary(auparse_state_t *au);
int auparse_normalize_subject_secondary(auparse_state_t *au);
int auparse_normalize_subject_first_attribute(auparse_state_t *au);
int auparse_normalize_subject_next_attribute(auparse_state_t *au);
int auparse_normalize_object_primary(auparse_state_t *au);
int auparse_normalize_object_secondary(auparse_state_t *au);
int auparse_normalize_object_primary2(auparse_state_t *au);
int auparse_normalize_object_first_attribute(auparse_state_t *au);
int auparse_normalize_object_next_attribute(auparse_state_t *au);
int auparse_normalize_get_results(auparse_state_t *au);
int auparse_normalize_key(auparse_state_t *au);
```

DESCRIPTION

After calling the **auparse_normalize** function, you will probably want to access the audit event data. These function provide access to the results of the normalization. There are 2 kinds of function, metadata and positioning.

The metadata functions all return a pointer to a string that describes something about the event. This data does not live inside the event but is kept in lookup tables inside the auparse library.

The positioning function are different in that they move the internal cursor of auparse to the record and field that contains the information you want. You then use field accessor functions to retrieve the values.

RETURN VALUE

The positioning functions return < 0 on error, 0 if uninitialized, and 1 on success. The metadata functions return NULL on error and a pointer to a string on success.

SEE ALSO

auparse_normalize(3), auparse_get_field_str(3), auparse_interpret_field(3).

AUTHOR

Steve Grubb