Trace Services and Audit in Firebird

Trace Services and Audit

- What is Trace Services
  - Trace Sessions
  - User trace sessions and Audit trace session
- How it works
- How to manage trace sessions
- How to use it in own applications
- Typical use cases
  - system audit
  - user trace

Trace Sessions

- Identification
  - ID, assigned by the engine
  - Name, optional and not unique
  - Created user name
  - Date and time of start of session
- Configuration
  - Traced databases and\or Firebird services
  - Traced events, details level and filters

Trace Sessions

- Scope
  - system administrator - traced all attachments
  - regular user - traced own attachments only
- State
  - running
  - suspended
- Output
  - trace session log file(s)

Trace Session Configuration

- Section <*database*>
  - default parameters for all databases
- Section's <*database pattern*>
  - specify parameters for database matching pattern
- Section <*service*>
  - default parameters for all services

Pattern is database\service name or regular expression with the syntax of SIMILAR TO predicate

Trace Session Configuration

- Section <*database*>
  - Connection and transaction related events
    - log_connections
    - connection_id
    - log_transactions
    - log_sweep

Trace Session Configuration

- Section <*database*>
  - SQL statement related events
    - log_statement_prepare
    - log_statement_free
    - log_statement_start
    - log_statement_finish
    - include_filter
    - exclude_filter
    - print_plan

Trace Session Configuration

- Section <*database*>
  - PSQL related events
    - log_procedure_start
    - log_procedure_finish
    - log_trigger_start
    - log_trigger_finish
    - log_context

Trace Session Configuration

- Section <*database*>
  - BLR API related events
    - log_blr_requests
    - print_blr
    - log_dyn_requests
    - print_dyn
  - Performance info logging
    - print_perf

Trace Session Configuration

- Section <*database*>
  - Various restrictions
    - time_threshold
    - max_sql_length
    - max_arg_length
    - max_arg_count
    - max_blr_length
    - max_dyn_length

Trace Session Configuration

- Section <*service*>
  - log_services
  - log_service_query
  - include_filter
  - exclude_filter

Trace Session Configuration

- Both <*database*> and <*service*> sections
  - enabled
  - log_filename
  - max_log_size
  - log_errors

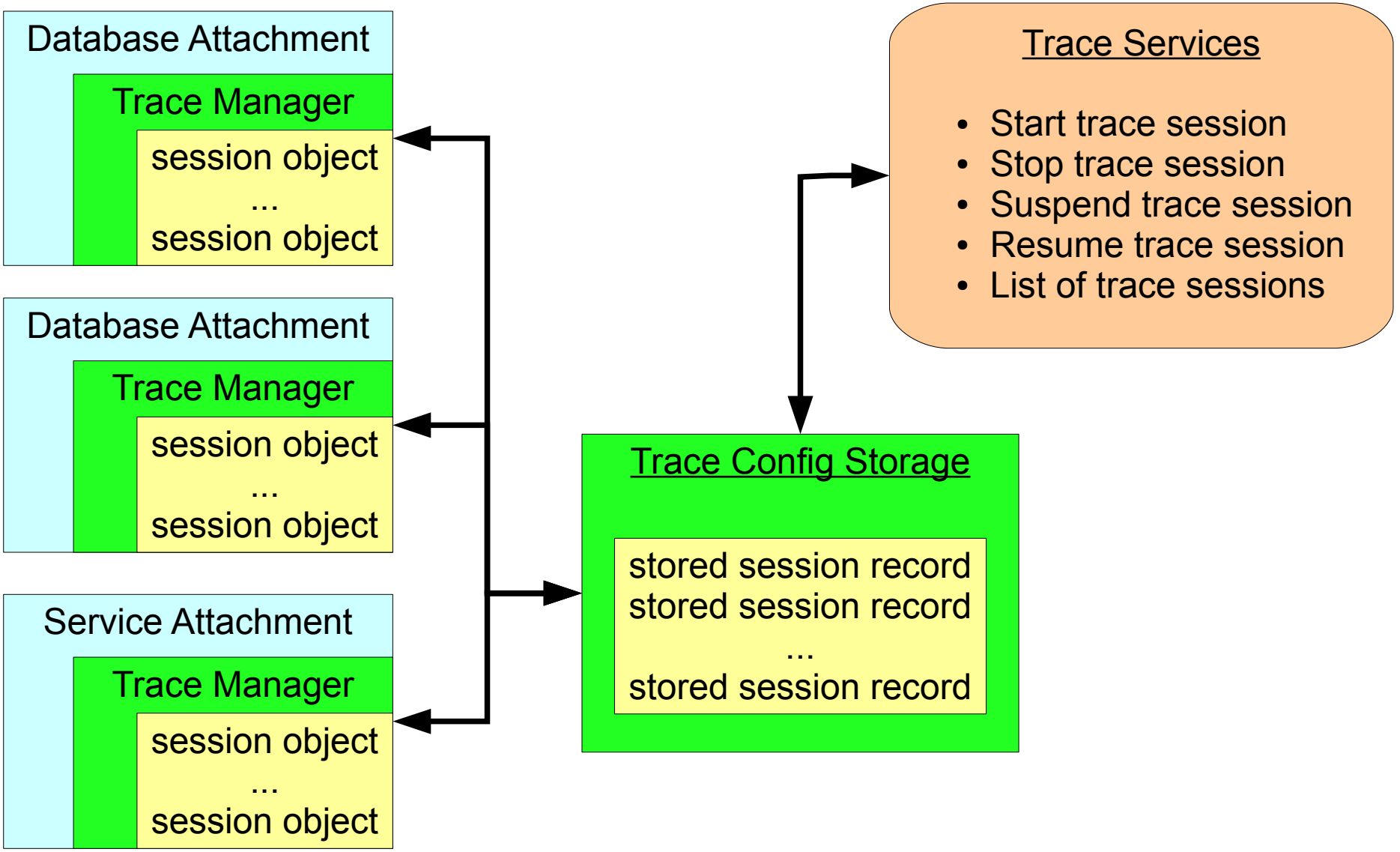
User Trace and System Audit

- User trace session
  - Initiated (started) by user via special service
  - Not preserved after Firebird shutdown
  - Output read by initiated service connection
  - Scope depends on user privileges
- Audit trace session
  - Initiated only by Firebird itself
  - Started with Firebird every time
  - Output stored in log file(s)
  - Scope is not limited

User Trace and System Audit

- User trace session
  - Could be temporary paused by the Firebird
  - Could be many user trace sessions
  - Could be managed by creator user or by SYSDBA
- Audit trace session
  - Never interrupted by Firebird
  - Only one audit trace session could exists
  - Could be managed by SYSDBA only

Trace Sessions in the Engine



Trace Config Storage

- Consists from two files
  - *fb_trace*, control file, mapped into shared memory
  - *fb_trace_AAAAAA*, storage of trace sessions records
- Both files placed at Firebird lock directory
  - by default COMMON_APPDATA\firebird
- Creates when Firebird process starts
- Shared by all Firebird processes (embedded too !)
- Deleted when last Firebird process gone
  - trace sessions is not preserved between Firebird restarts

Trace Config Storage

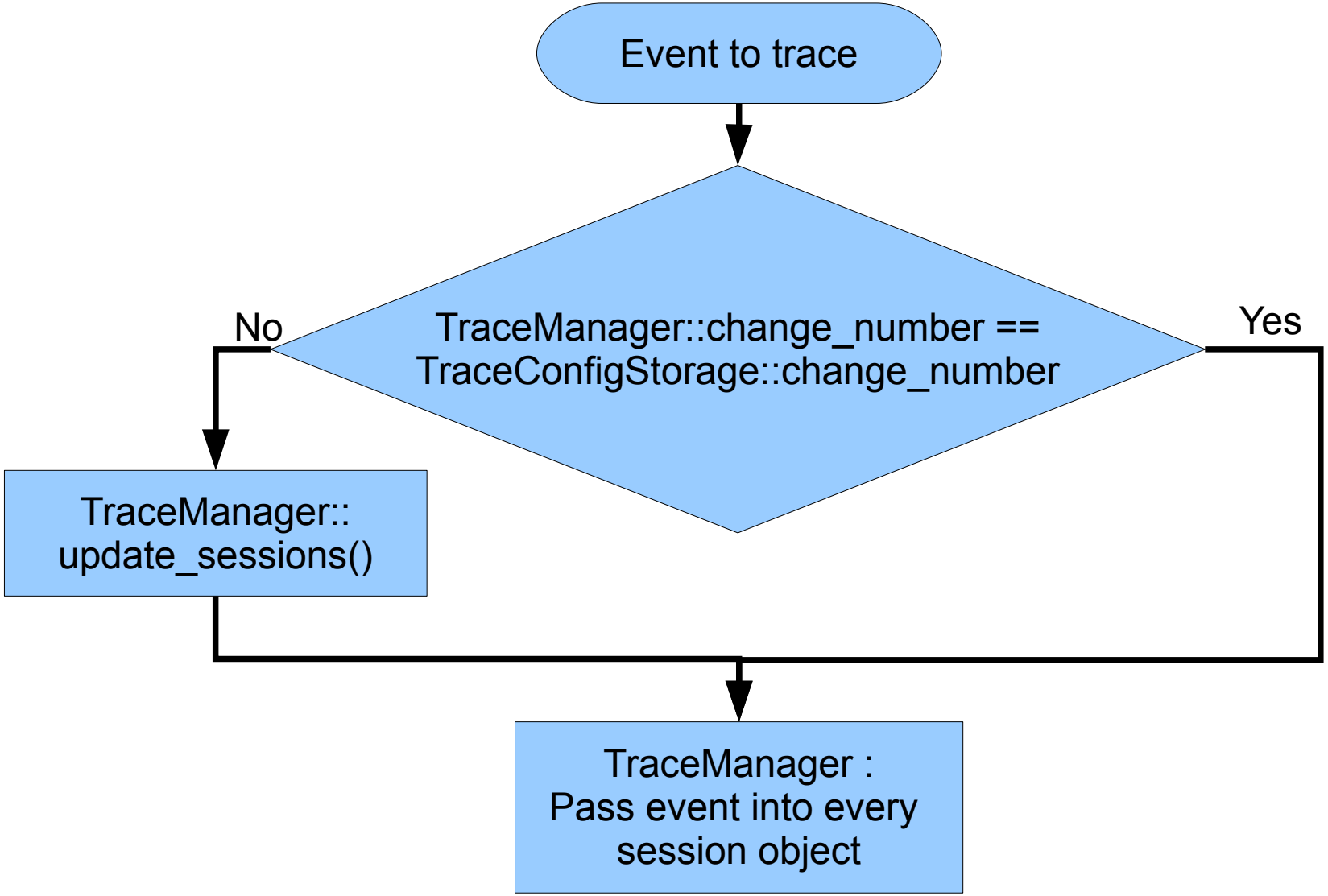
Control File
fb_trace

```
struct ShMemHeader
{
   ULONG version;
   volatile ULONG change_number;
   volatile ULONG session_number;
   ULONG cnt_uses;
   char  cfg_file_name[MAXPATHLEN];
...
}
```

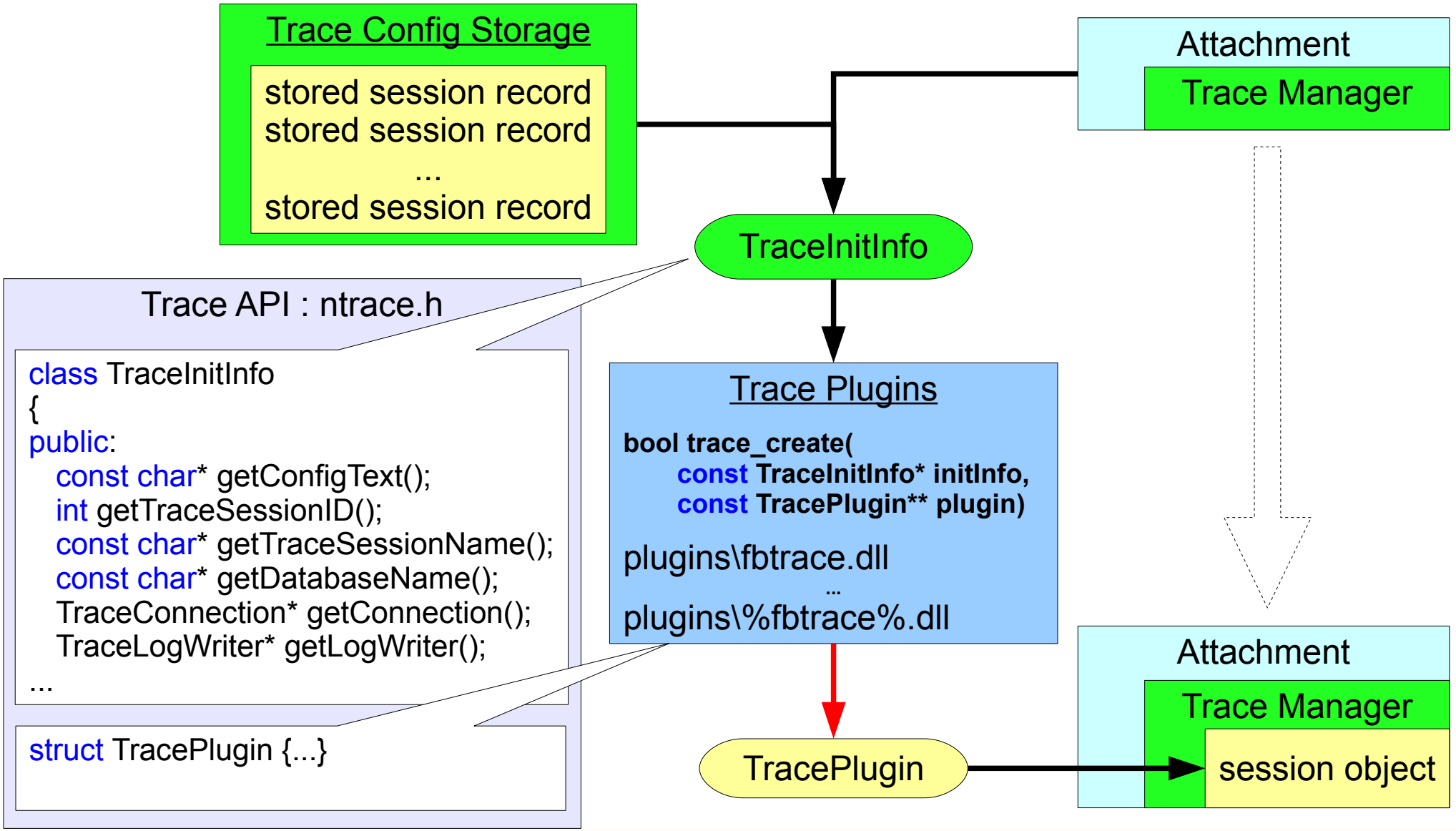
Config Storage File
fb_trace_AAAAAA

stored session record
stored session record
...
stored session record

Trace Manager



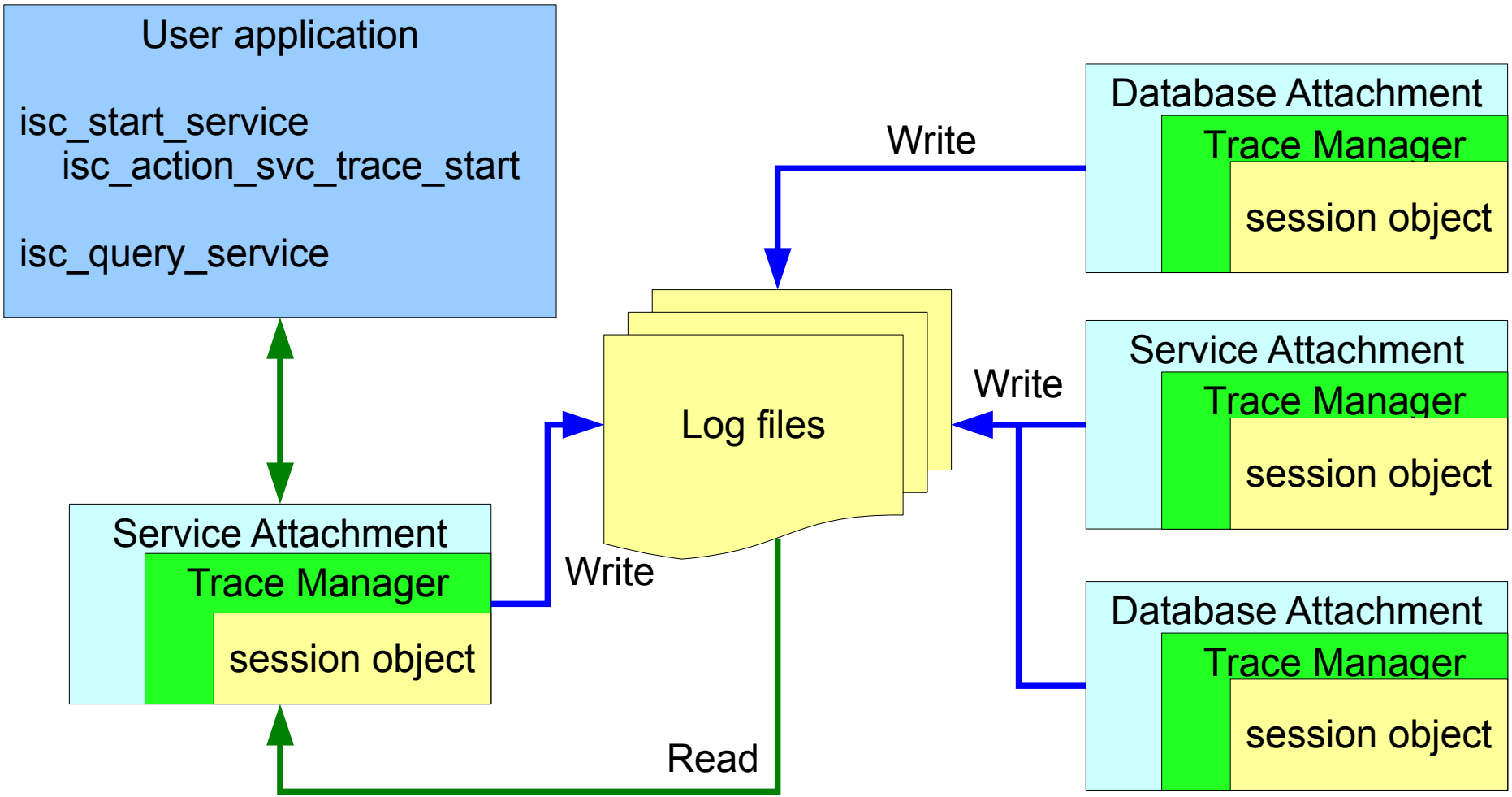
Session object in Engine



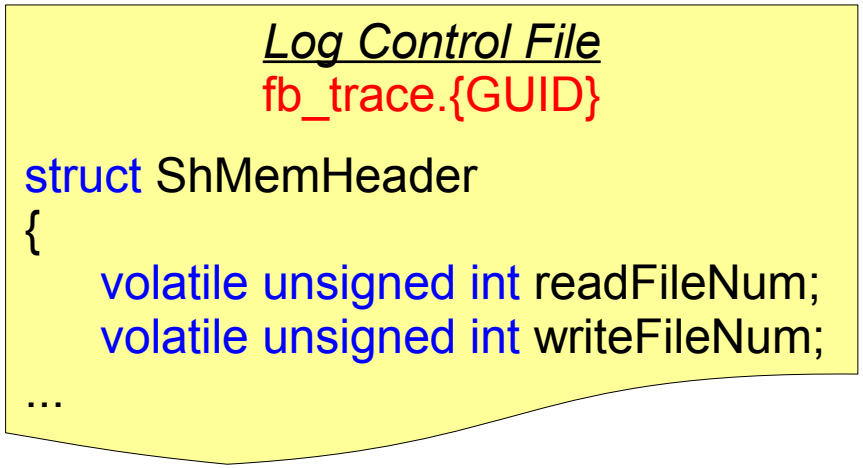
Trace session's output

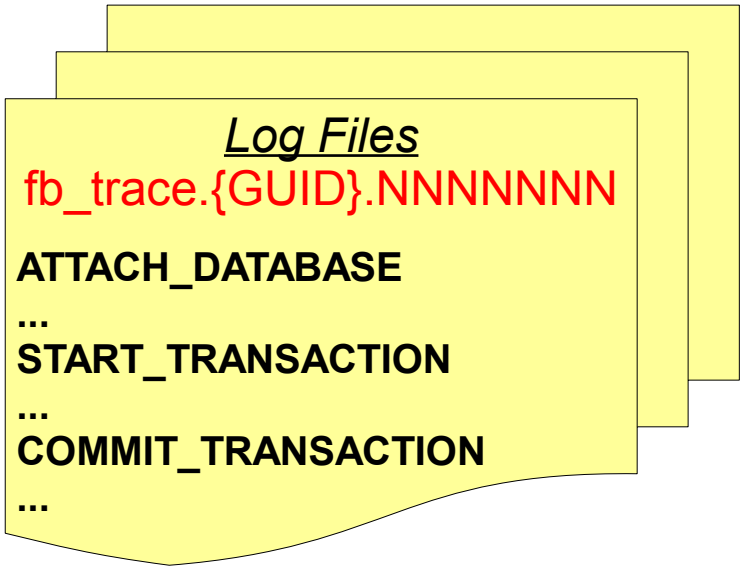
- User trace
  - Many writers
  - One reader
  - Disk space released while reading
  - Delete whole log when reader gone
  - Log file name set by Firebird
- System audit trace
  - Many writers
  - No readers
  - Log files rotation
  - Log files not deleted by Firebird
  - Log file name set in trace configuration on per-database (service) basis

Output of user trace



Output of user trace





- Log files placed at Firebird's lock directory
  - by default COMMON_APPDATA\firebird
- Maximum size of each log file is 1MB
- Maximum summary log size set in firebird.conf
  - MaxUserTraceLogSize = 10

Output of System Audit trace

- Stored in disk file(s)
- File name set in trace configuration file on per-database (per-service) basis
  - «log_filename» setting in <database> or <service> section
  - Each traced database or service could have own trace log file
- Each log file could be rotated when its size reached «max_log_size» MB

How to manage trace sessions

- New utility «fbtracemgr» is introduced
- It allows to
  - Start user trace session and read its output
  - Stop any trace session
  - Suspend and resume any trace session
  - Obtain a list of existing trace sessions
- SYSDBA allowed to manage the trace sessions of any user
- Non-SYSDBA allowed to manage own trace sessions only

Trace Services in own Applications

- For every Trace task there is corresponding Firebird service
  - isc_action_svc_trace_start
  - isc_action_svc_trace_stop
  - isc_action_svc_trace_suspend
  - isc_action_svc_trace_resume
  - isc_action_svc_trace_list

THANK YOU FOR ATTENTION !

Questions ?

Firebird official web site

Firebird tracker

hvlad@users.sf.net