A string representing a UTC value in YYYY-MM-DD hh:mm:ss format indicating the date and time when the audit event was generated. For example, the event corresponding to execution of an SQL statement received from a client has a timestamp value occurring after the statement finishes, not when it was received.

Example:

```
"timestamp": "2019-10-03 13:50:01"
```

For audit records that have the same timestamp value, their id values distinguish them and form a sequence. Within the audit log, timestamp/id pairs are unique. These pairs are bookmarks that identify event locations within the log.

These items appear within hash values associated with top-level items of JSON-format audit records:

• args

An array of options that were given on the command line or in option files when the MySQL server was started. The first option is the path to the server executable.

Example:

• command

A string representing the type of instruction that generated the audit event, such as a command that the server received from a client.

Example:

```
"command": "Query"
```

connection_type

The security state of the connection to the server. Permitted values are tcp/ip (TCP/IP connection established without encryption), ssl (TCP/IP connection established with encryption), socket (Unix socket file connection), named_pipe (Windows named pipe connection), and shared_memory (Windows shared memory connection).

Example:

```
"connection_type": "tcp/tcp"
```

• db

A string representing a database name. For connection_data, it is the default database. For table_access_data, it is the table database.

Example:

```
"db": "test"
```

• host