Auditing

On this page

New in version 2.6.

MongoDB Enterprise includes an auditing capability for `mongod` and `mongos` instances. The auditing facility allows administrators and users to track system activity for deployments with multiple users and applications.

Enable and Configure Audit Output

The auditing facility can write audit events to the console, the syslog, a JSON file, or a BSON file. To enable auditing for MongoDB Enterprise, see Configure Auditing.

For information on the audit log messages, see System Event Audit Messages.

Audit Events and Filter

Once enabled, the auditing system can record the following operations:

- schema (DDL),
- replica set and sharded cluster,
- authentication and authorization, and
- CRUD operations (requires `auditAuthorizationSuccess` set to `true`).

For details on audited actions, see Audit Event Actions, Details, and Results.

With the auditing system, you can set up filters to restrict the events captured. To set up filters, see Configure Audit Filters.

Audit Guarantee

The auditing system writes every audit event [1] to an in-memory buffer of audit events. MongoDB writes this buffer to disk periodically. For events collected from any single connection, the events have a total order: if MongoDB writes one event to disk, the system guarantees that it has written all prior events for that connection to disk.

If an audit event entry corresponds to an operation that affects the durable state of the database, such as a modification to data, MongoDB will always write the audit event to disk *before* writing to the journal for that entry.

That is, before adding an operation to the journal, MongoDB writes all audit events on the connection that triggered the operation, up to and including the entry for the operation.

These auditing guarantees require that MongoDB run with `journaling` enabled.

> **WARNING:**
> MongoDB may lose events **if** the server terminates before it commits the events to the audit log. The client may receive confirmation of the event before MongoDB commits to the audit log. For example, while auditing an aggregation operation, the server might crash after returning the result but before the audit log flushes.

[1] Audit configuration can include a filter to limit events to audit.