MongoDB Community Server itself doesn't have a built-in audit logging feature. However, the CIS benchmarks might still offer recommendations for achieving a level of auditability on Ubuntu using alternative approaches:

1. External Syslog Integration:

- Configure MongoDB to send log messages to a centralized syslog server on your Ubuntu system. This allows collecting and analyzing logs from various sources, including MongoDB, for potential security events.
- Tools like rsyslog can be used to manage syslog on Ubuntu.

2. Third-Party Auditing Solutions:

- Consider implementing third-party security or auditing solutions that integrate with MongoDB. These solutions might offer features to capture user activity, database operations, and security events within MongoDB.
- Evaluate available solutions based on your specific needs and budget.

3. Database Activity Monitoring Tools:

- Explore open-source or commercial database activity monitoring (DAM) tools that can connect to MongoDB and track user actions. These tools can provide insights into database operations and potential suspicious activity.

4. Custom Scripting (Optional):

- For advanced users, creating custom scripts that interact with the MongoDB command-line interface (CLI) might be an option. These scripts could periodically capture information about user activity or database changes and store them in a central location for analysis.

5. Leverage Existing Monitoring Tools:

- If you already have monitoring tools in place for your infrastructure, explore their capabilities for capturing data relevant to MongoDB activity. Some monitoring tools might integrate with MongoDB or offer custom scripting options to collect audit data.

Here's a general approach for integrating MongoDB with syslog on Ubuntu:

1. Install and configure rsyslog on your Ubuntu system.
2. Edit the MongoDB configuration file (/etc/mongodb.conf).
3. Add a section for logging:

YAML

```
systemLog:
  destination: syslog
  logAppend: true
  logRotate: hourly
  logLevel: verbose
```

- This configuration sends logs to the syslog server, appends new entries instead of overwriting, rotates logs hourly, and sets the log level to verbose (adjust based on your needs).

4. Restart the MongoDB service.

Remember:

- These are alternative approaches since MongoDB Community Server lacks built-in audit logging.
- Evaluate the trade-offs between complexity, available resources, and achieving a desired level of auditability.
- Regularly review logs and implement additional security measures like strong authentication and authorization to enhance overall security.

Additional Resources:

- CIS MongoDB Security Benchmarks (reference security guides that mention them): While not available directly online, you can find references and explanations in security guides that reference CIS benchmarks. Search for "CIS MongoDB Security Benchmarks Ubuntu".
- Ubuntu Documentation on Rsyslog: https://manpages.ubuntu.com/manpages/xenial/en/man5/rsyslog.conf.5.html
- MongoDB Documentation on System Logs (for reference): https://www.mongodb.com/docs/manual/reference/log-messages/