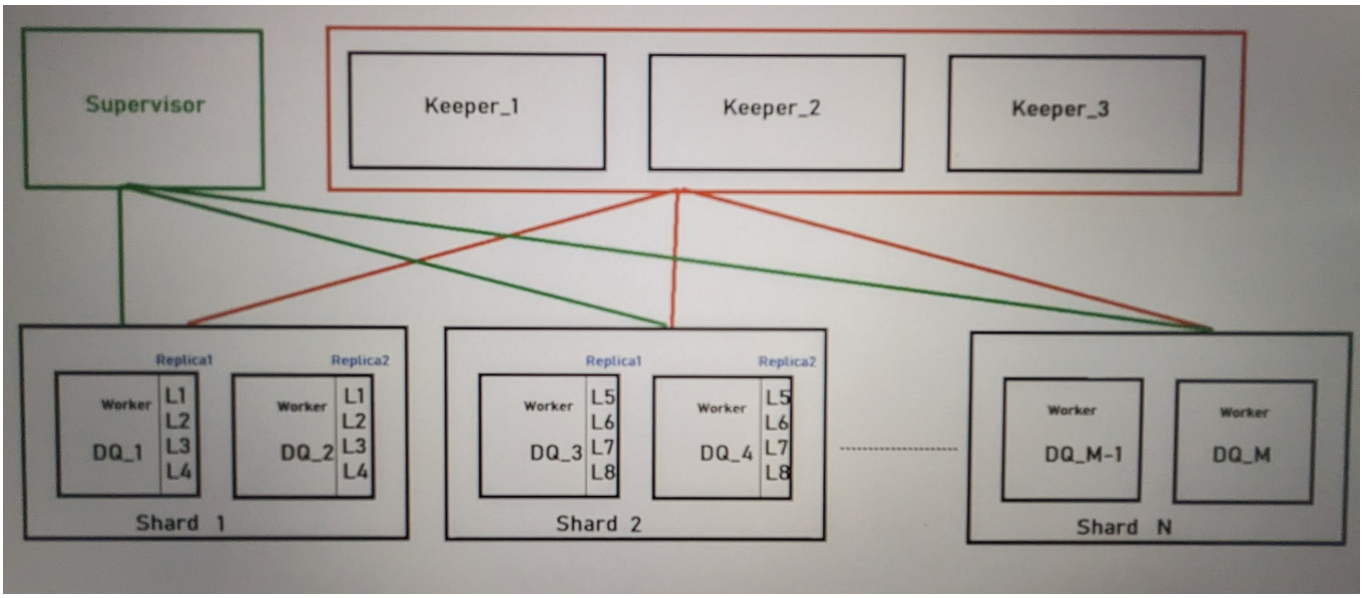
Note:

- FortiSIEM Sizing Guide - ClickHouse

- `Clickhouse` is the best option and fortinet encourage all customers to migrate their existing database like `Elasticsearch` or `Event DB` to `Clickhouse`

- There are some clickhouse specific roles (2 roles - `Keeper role` and `Data query role`)
  - when you design your `clickhouse cluster`, you have to distribute the roles among different workers



Note:

- `Shard` - It's just a logical entity means, that you divide the database of the events among different clusters. this will enhance the performance and the processing of the database.
  - e.g., if you have the database of 8 logs, so instead of putting all the logs in one shard or one cluster, we distribute among two clusters. (we are dividing among 2 so the `replication factor` is 1)

- N (Shard) = M/2 (Workers)

- `Keeper` - Are responsible for replication and also locating the right `shard` with the right `workers` that have log.

- so when you access the UI as a analyst, the query that you initiate for searching will come to the `keepers`, the keepers will look up their index and define the `shard` to have information. so it will look up only specific `shard` instead of whole database.

- for example, if the `DQ_3` is down, the `Replica2` will do the job