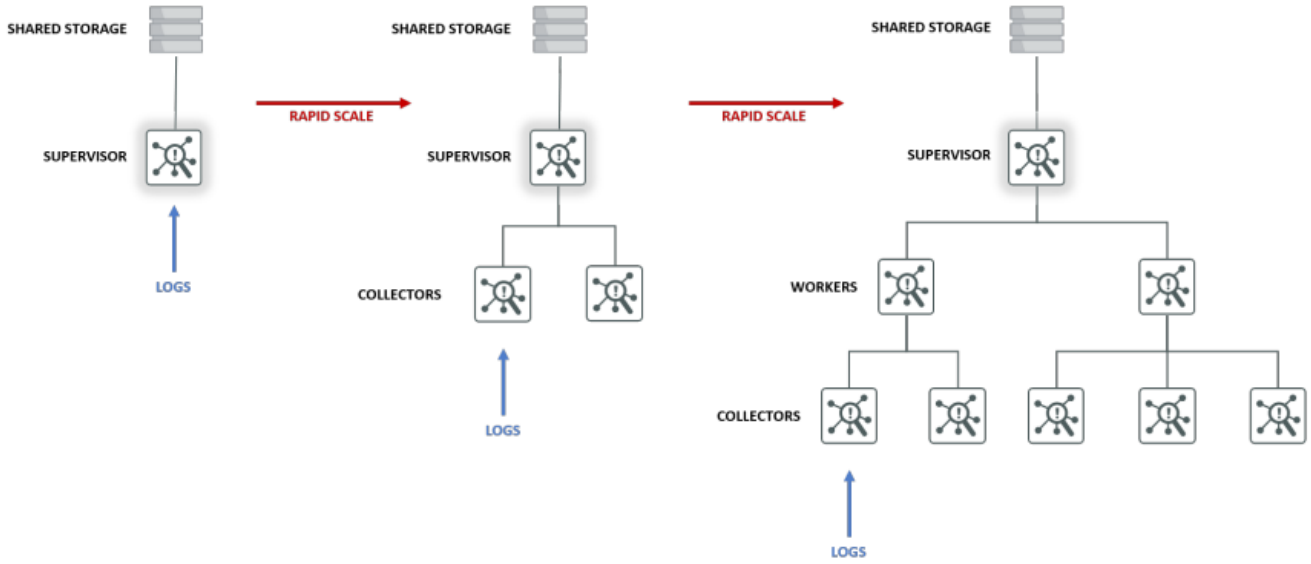
Note:

- Reference Architecture (is not including Clickhouse DB opiton)
  - Rapid Scale Architecture: The Rapid Scale Architecture allows FortiSIEM to scale quickly and easily from a small single Supervisor node to a massive distributed system processing huge log volumes. This scalability is achieved with a distributed architecture utilizing a common supervisor node, with additional worker and collector nodes as required for scalability.
    - `workers` - Is a middle layer between the supervisor and the collector and you actually bring them here in case you need to have a very big environment with a very high EPS and then the load will be too high for the supervisor to carry out alone. so you need to bring some assistant to supervisor



FortiSIEM Rapid Scale Architecture

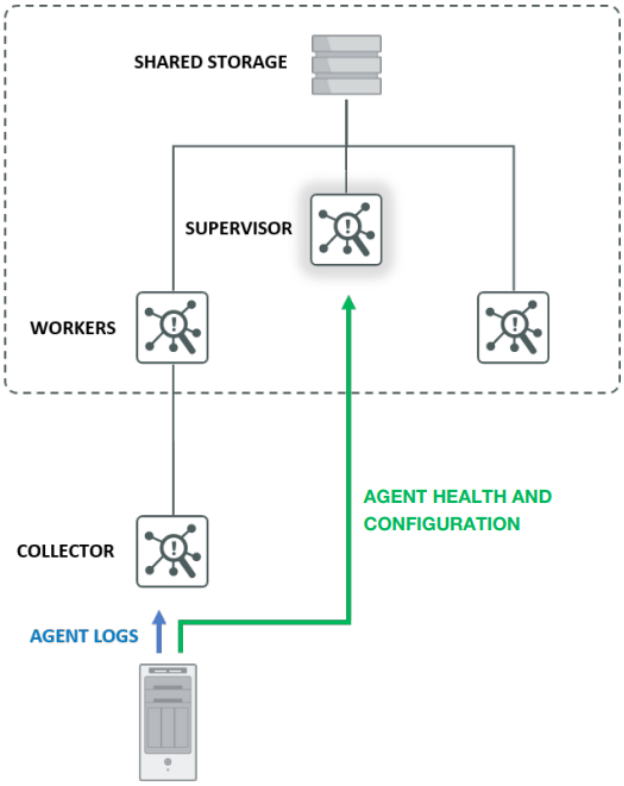
- SIEM solution has 2 main functions (`collection layer` and `correlation layer`)
- In first two FortiSIEM architecture, the supervisor were carrying out the functions and the corellation and processing functions of the logs and the storage of the logs into the database.
- But, In third architecture, we offload all processing correlation to the `workers`. So the supervisor will be focusing only on the UI functions to access the interface and also storing the some database, not all the database (say only `CMDB database` (for storing NOC information), other (`SVN database` and `Event database`) will be stored by workers)
- `Supervisor` will have the complete visibility

- for example, if we have a brute force login attempts, but not all the login attempts are coming to collector number one, say we have 3 failures coming to collector one and two failures coming to collector four. In this case, the worker one will do the partial match because if the rule is checking five failures in one minute, only 3 failures are coming here. for worker number two, two failures are coming from collector 4. the supervisor will be able to connect the dots and trigger the alert. this is the beauty of the architecture.

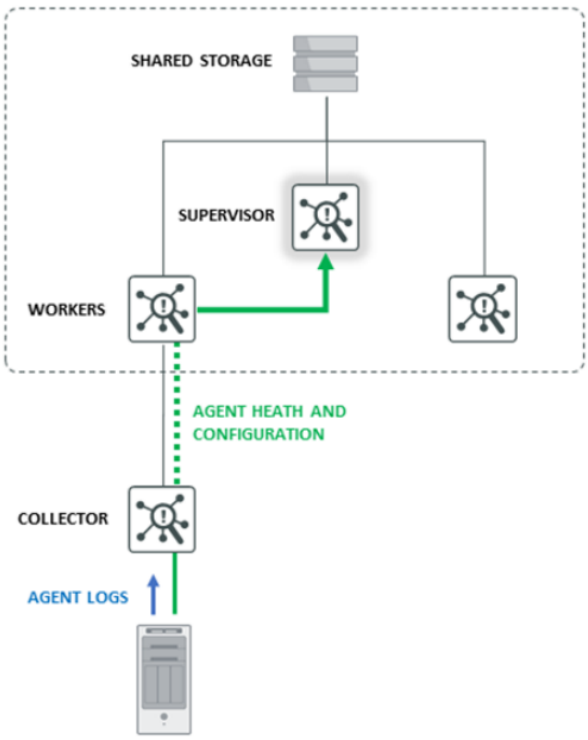
- always have a `shared storage` in case you need to expand from small scale to large scale. in first two cases we don't need shared storage, but if you planning to expand in the future, it's best practice to have a shared storage outside the supervisor node. - best suited for `event database` or `elasticsearch`
  - For `clickhouse` (internal database - which is distributed among the workers and the supervisors) database, this requirement not required, we don't need to worry about the external storage because all nodes will have their own embedded clickhouse database.

NOTE:

- basically `supervisor` is the manager of different components (workers, collectors, agents, etc.). we need to register everything with the supervisor. for example, after installing workers you need to register workers with the supervisor. then supervisor can load balance among the workers
- supervisor is responsible for maintaining the health of the agent (by default, it is going directly to the supervisor without passing by any other nodes. but there is a option to change this behaviour and use the collector as a proxy to relay the health checks to the supervisor - this is mandatory for MSSP setups, because each agent is connected with one customer only)



FortiSIEM Agent Collector Architecture (Direct)



FortiSIEM Agent Collector Architecture (Proxy)

Designing the event database

- FortiSIEM combines four back end databases into a single GUI for a seamless user experience.
- The databases are:

Component	Description
Profile Database	Stores risk data and system data
SVN	Stores device configuration data
CMDB	Stores data relating to the FortiSIEM internal CMDB
Event Database	Event storage

- The profile database, SVN and CMDB are hosted on the Supervisor node in all deployment types.
- The event database design must be considered in all deployments. The event database can be hosted on one of three locations:
  - `Local (all-in-one deployment)
  - `NFS shared storage`
  - `Elasticsearch`

Note:

- when you design or size your solution, you have to consider the retention days on `online` and `archive`.