Cluster controller (CC) acts as the failure monitor of all the worker processes in the cluster. All the workers heart beats to the cluster controller to report their health. If the cluster controller (CC) marks a worker as failure if it doesn't receive heartbeats for a specified amount of time. This time is set using the knob WORKER_FAILURE_TIME and it's default value is 1 sec. Storage servers have a different timeout and will be explained later.

When the CC detects failure of stateless or TLog worker, it triggers a recovery process by which new stateless (proxy, resolver, etc.,) and TLog workers are recruited and a new generation is started. Storage server failures do not trigger recovery but data distribution gets triggered to move the data off the failed storage server to other storage servers and also rebalance data.

For the purpose of data distribution, failure of a storage server worker is determined with a different timeout knob DATA_DISTRIBUTION_FAILURE_REACTION_TIME which is generally higher. The default value is 60 seconds. If the storage server comes back after it is marked as failed, there are two cases to handle. If all data has been re-replicated, then the data files will be deleted and it will start fresh. Otherwise, the storage server will retain its data files and maintain responsibility for any data that hadn't yet been re-replicated. It's possible that this is only a small portion of the original data assigned to that process, in which case much of the file will be unused and have to be reclaimed for reuse. Additionally, the cluster will attempt to move new data onto this process to replace data that had been moved away in order to keep the logical amount of data stored on each process balanced.