Fault Tolerance Documentation

**<REDACTED>– <REDACTED>– James Ryan – <REDACTED>**

University of Victoria

SENG 468

# General Failures of Servers

Docker compose provides the ability to automatically detect failures in system components and restart them based on parameters set. This functionality has not been enabled at this stage of development, however in a real-world situation we would ensure it was enabled for production environment deployments of the system.

# On a failure of a Transaction Server

On failure of a transaction server, the web server will detect that the transaction server is no longer accessible and create a new connection to a different transaction server through HAProxy. This then allows the clients who are connected to that web server to continue their sessions on our platform with the minimal delay and error possible.

HAProxy will also detect the failure of the transaction server and will not route any future connections to transaction servers from web servers to that transaction server.

# Improvements

To improve the system, we do have to address the fact that the logs are being stored on each individual server’s local hardware, rather than a distributed cloud database. In the event of a hardware failure, the logs stored on that device would be lost, unless we had backups of each server’s hard drive, which would be very costly and not distributed. To improve this, we need to put the logs into a separate database that is distributed in a Docker container, however, this will impact performance. We found during development that logging every transaction was our most significant bottleneck for achieving faster transactions per second.