Reliability and recoverability

Non-Functional Requirements

Backups of company data and app information should be taken at regular intervals

Creating regular backups of critical information allows us to revert to an earlier version of our software in case of a failure

Backups of user data should be stored frequently

Backups of user data should be done frequently to avoid any data loss. A loss or corruption of user data would negatively impact their experience and could potentially cause further problems. It is important to store a recent copy of user information. Servers should be distributed

Storing all the critical servers in the same place leaves the servers vulnerable to power failures, natural disasters, and other problems which could cause all the servers at a specific location to become inoperable.

Servers should fail as little as possible

Servers should be set up with reliability in mind, as crashes could cause slowdowns and data loss, as well as cause outages and further problems with other servers.

In case of a failure there should be no data loss

The infrastructure should be planned with the goal of minimizing data loss and data corruption, as these issues are likely to cause further problems with other parts of the application.

Servers should be able to quickly recover from failures

In case of a failure servers should be able to quickly restart and recover, and appropriate staff members should be notified of crashes, outages and problems.

Functional Requirements

Hashes and checksums of stored and sent data should be taken and checked

To prevent data corruption during transfer and storage of information data should be hashed and check summed.

Server load should be distributed across multiple servers, and in case of a server failure it should be redistributed to the working servers.

Load balancing allows for easily redistributing the user connections to working servers in case of a server failure, allowing the entire network to stay working at all times.

Backups should follow the 3-2-1 backup rule

Backup servers can fail, and it is possible for the disks which store the backups to be damaged or lost, which is why it is important to store backups in several places at once. The 3-2-1 rule states that to minimize the chances of a backup being completely lost, 3 copies of it should be stored on-site, 2 copies should be stored off-site, and 1 copy should be stored with an external provider. This is to prevent on-site copies from being lost, and software problems making on-site and off-site backups inaccessible.

References

Wikipedia Contributors (2019). *Backup*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Backup.