Server Design Specification

Riley Poole
Golden Ticket Engineering, LLC

November 29, 2025

Contents

Chapter 1

Objectives

Chapter 2

Disaster Recovery

2.1 Failover

There are to be three servers: a production server, a backup server, and a failover server. The production server will be used for the everyday tasks and use of the system. On a regular and frequent basis the production server will back up a Zettabye Filesystem (ZFS) snapshot to the backup server. The backup server stores this snapshot in it's own ZFS system and relays it to cloud storage such as Azure S3 or equivilent offsite cloud storage. The failover server, at the same frequency, will load and run the most recent snapshot. In this configuration, one server is running, one server is ready for failover, and there are two locations of backups. At any one time there are four copies of the state of the system, two of which are ready for deployment, and one is already deployed. The frequency of the snapshots is discussed in subsection 2.1.2.

2.1.1 Backup Terminology Review

Throughout this document the term *backup* is meant to mean any saved data which can be used to independently restore itself. It is the most general and abstract idea of file redundancy. How a backup is made is significant to the risk profile. As such it is important to distinguish between the various types of backup. However, note that in the context of this document, a backup is mean to mean a saved state of the system. The consideration of individual files is not made. This is because the availability of the entire system is prioritized. That is the availability uptime of every file and service at once.

Image An image is the direct copy, bit by bit, of a drive or partition. It is the most complete form of backup. From it another identical drive or partition can be made. It has the lowest risk profile because it is totally independent of other components. It can almost always be read, unless encrypted, although it may not boot.

Snapshot vs Incremental Snapshot A snapshot is an instantanious copy of a drive at an instant. They are excellent in the use case of rolling back to a previous state. Say for example, the hour before a crash. Care should be used not to confuse it with an image. They are used in the context of virtual machines and virtual filesystems. Examples include .vdi extensions and the ZFS filesystem. It may be an independent snapshot or it may be incremental. What is important is that the risk profile is higher with incremental snapshots as they may depend on a chain of snapshots.

Restore Point and Shadowcopy These are the Windows equivilents of incremental snapshots. Windows NTFS filesystems do not have the concept of snapshot outside of Windows virtual machines. This terminology will not be used in this document, as the systems to be built will be Linux based. They have a higher risk profile than incremental snapshots because they are proprietary and often tied to the hardware configuration, OS, or user data. They may require an activated account or other authentication to allow them to be be booted from or mounted during a live boot.

2.1.2 Backup Retention Policy

An incremental snapshot will be made every hour on the production server and sent via SSH to the backup server. The backup server will then upon receipt send that copy via SSH to an Azure Ubuntu virutal machine which utilizes S3 storage. The backup server will send via SSH the new snapshot to the failover server. A backup will be made every hour, day, week, month, and year. In decreasing levels of risk profile. The retention policy shall be:

- 24 hourly incremental snapshots
- 7 daily full snapshots
- 4 weekly full snaphots
- 12 monthly full snapshots
- Annual full snaphot