容错, 高可用和灾备

原创 阮一峰 阮一峰的网络日志 2019-11-17

标题里面的三个术语,很容易混淆,专业人员有时也会用错。本文就用图片解释它们有何区别。



容错^[1](fault tolerance)指的是, 发生故障时,系统还能继续运行。

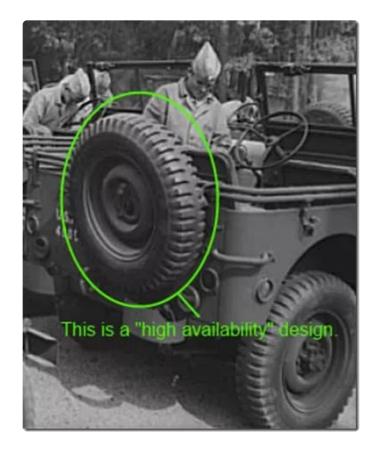


飞机有四个引擎,如果一个引擎坏了,剩下三个引擎,还能继续飞,这就是"容错"。同样的,汽车的一个轮子扎破了,剩下三个轮子,也还是勉强能行驶。

容错的目的是,发生故障时,系统的运行水平可能有所下降,但是依然可用,不会完全失败。

高可用

高可用^[2](high availability)指的是, **系统能够比正常时间更久地保持一定的运行水平。**



汽车的备胎就是一个高可用的例子。如果没有备胎,轮胎坏了,车就开不久了。备胎延长了汽车行驶的可用时间。

注意,高可用不是指系统不中断(那是容错能力),而是指一旦中断能够快速恢复,即中断必须是短暂的。如果需要很长时间才能恢复可用性,就不叫高可用了。上面例子中,更换备胎就必须停车,但只要装上去,就能回到行驶状态。

灾备

灾备^[3](又称灾难恢复,disaster recovery)指的是, 发生灾难时恢复业务的能力。



上图中, 飞机是你的 IT 基础设施, 飞行员是你的业务, 飞行员弹射装置就是灾备措施。一旦飞机即将坠毁, 你的基础设施就要没了, 灾备可以让你的业务幸存下来。

灾备的目的就是,保存系统的核心部分。一个好的灾备方案,就是从失败的基础设施中获 取企业最宝贵的数据,然后在新的基础设施上恢复它们。注意,灾备不是为了挽救基础设 置,而是为了挽救业务。

总结

上面三个方面可以结合起来,设计一个可靠的系统。

• 容错: 发生故障时, 如何让系统继续运行。

• 高可用: 系统中断时, 如何尽快恢复。

• 灾备:系统毁灭时,如何抢救数据。

参考文献

• The Difference Between Fault Tolerance, High Availability, & Disaster Recovery^[4], Patrick Benson

References

- [1] 容错: https://en.wikipedia.org/wiki/Fault_tolerance
- [2] 高可用: https://en.wikipedia.org/wiki/High_availability
- [3] 灾备: https://en.wikipedia.org/wiki/Disaster_recovery
- [4] The Difference Between Fault Tolerance, High Availability, & Disaster

Recovery: http://www.pbenson.net/2014/02/the-difference-between-fault-tolerance-high-availability-disaster-recovery/

阅读原文