

Introduction

Public and Private Cloud Computing technologies have been marketed in recent years with the promise of achieving high availability and scalability without having to care any longer on system operation details or on software architecture. Both promise are often an illusion, soon enough discovered for scalability but discovered too late for data availability. The fake sense of confidence brought by Cloud Computing infrastructures has lead more than half of the companies we are in direct contact with to lose critical data of applications such as accounting, banking, trading, etc. In each of the case related to private Cloud which we are aware of, data loss was not revealed to the public, which prevented any know how sharing to improve overall IT security. However, incidents which happened in summer 2012 to Amazon (Europe) and Firstserver (Japan) highlight a dramatic increase of data losses in public Clouds, with deadly consequences on businesses which rely on Cloud.

The goal of this white paper is to define the risks of disaster posed by Cloud Computing and analyze the different solutions to mitigate those risks. In the first chapter, we categorize Cloud disaster scenarii based on real disaster cases and on theoretical cases. In the second chapter, we debunk the illusion that Cloud disaster risks can be mitigated by leaving the problem to the Cloud provider, to the disk bay provider or to a centralized business continuity provider. In the third chapter we introduce an approach to disaster recovery based on automated testing of well defined usage scenarii. In chapter four, we introduce a case study for a POSIX based ERP. In chapter five, we introduce a case study for a Windows based application. And in chapter six, we introduce a case study for a Software as a Service (SaaS).

Overall, this white paper highlights the 2 essential criteria for a resilient business continuity plan: it must be daily tested and it must be deployed on a decentralized infrastructure. Both criteria can be reached quite simply with recent technologies.