Disaster Recovery

A disaster is an unexpected event in a system lifetime. It can be made by nature (like the tsunami and earthquake), hardware/software failures (e.g. , VMs' failure of Heroku hosted on Amazon EC2 on 2011) or even human (human error or sabotage). It can lead to serious financial loss or even can put human lives at risk (Kashiwazaki., 2012). Hence, between 2% and 4% of IT budget in huge companies is expended for DR every year (Prakash et al., 2012). Cloud-based DR solution is an increasing trend because of its ability to tolerate disasters and to achieve the reliability and availability. It can be even more useful in small and medium enterprises (SMEs), because they do not have much resources as big companies do.

DR level with Description

- Data level -Security of application data
- System level -Reducing recovery time as short as possible
- Application level -Application continuity

DR mechanisms must have five requirements for an efficient performance (Wood et al., 2010):

- Have to minimize RPO and RTO
- Have a minimal effect on the normal system operation
- Must be geographically separated
- Application must be restored to a consistent state
- Must guarantee privacy and confidentiality

Disaster Recovery Plan

There are different DR approaches to develop a recovery plan in cloud system. They are based on the nature of the system. However in the literature, all these approaches are based on redundancy and backup strategies. The redundancy strategy uses separated parallel sites which have the ability to start up the applications after a disaster; whereas backup strategy uses replication technology (Lwin and Thein, 2009). The speed and protection degree of these approaches depend on the level of DR service that is shown in Table 5(Guster and Lee, 2011). In addition, three different types of replication technology are available:

1. Host and VM replication.
2. Database replication.
3. Storage replication.

Cloud-based DR models

Model	Synchronize time	Recovery time	Backup characteristics	Tolerance support
Hot	Seconds	Minutes	Physical mirroring	Very high
Modified Hot	Minutes	1 hour	Virtual mirroring	High
Warm	Hours	1-24 hours	Limited physical mirroring	Moderate
Cold	Days	More than 24 hours	Off site backup	Limited

The objective of disaster recovery planning is to minimize RTO, RPO, cost, and latency by considering system constraints such as CPU, network and storage requirements. So we can say DR recovery planning can be considered as an optimization problem. According to (Nayak et al., 2010), DR plans include two necessary phases:

- Matching Phase: In this phase, all DR solutions have to be matched to the requirements of any data container (a data container means a data set with identical DR requirements)
- Plan composition phase: Selecting an optimal DR solution which can minimize cost with respect to required QoS for each data container.ENDEAVOUR (Nayak et al., 2010) is a framework for DR planning process.It consists three modules:

1. Input modules: Including DR requirements (such as protection type, RTO, RPO and application latency), Discovery engine (To find configuration information of primary and secondary sites) and knowledge repository (Replication technologies, instructions and composition formula).
2. Planning Modules: Including solution generation (Analyzing DR requirements and matching them to replication techniques), Ranking (Sorting DR plans in terms of some attributes like cost, risk and latency (Azagury et al., 2002)) and Global optimization (selecting an optimal DR plan (Jaiswal et al., 2011)).
3. Output: The output of ENDEAVOUR is an optimal DR plan for each application with some details like: target resources and devices, replication protocol configuration.