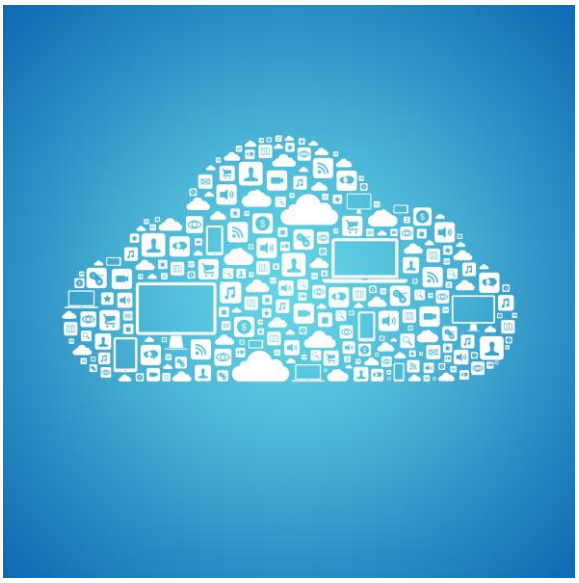
NebuLogic
Cloud Computing Delivered ©

Whitepaper

Cloud Disaster Recovery: Five Key Steps to Avoid Risk and Secure Your Data.

Contents



Hosting applications on the cloud is tempting many IT organizations for sundry reasons like availing benefits from outsized datacentres, backup power sources and other capabilities that till lately only established IT organizations could afford. Pay-as-you-go culture or guaranteed availability makes cloud adoption an easy and unperturbed choice for many SMBs and large scale organizations.

Many hosting providers maintain compound data centres, so decision makers often assume disaster recovery to be the inherent feature in the cloud culture that is offered to them. But little do they realise that this is a vital issue that warrants concern. Disaster Recovery (DR) is not a default configuration for many providers that offer cloud space in the IT market.

As technological fluctuations will go round the world, cloud providers will likely be on the buying or selling side of the data center acquisition or integration. Most important part lies in evaluating and selecting the right service provider with the right Disaster Recovery strategies, equally important is the step to review your DR requirements and solutions.

The 9/11 attacks cautioned many towards IT disaster preparedness (though probability of such disasters are extremely rare but not impossible). Before dealing with your cloud space provider and before signing on the dotted line, the DR diligence should be thoroughly assessed. The thought process should determine the risks, lay out the potential solutions and implement the plan that meets the required service level at reasonable costs.

Hereby, this paper discusses the storage elements of Disaster Recovery Planning process.

Step 1: Risks Assessment/ Evaluating the Risks

Disaster risks can be perceived as a range of probability. They can be categorized into three major groups:

- **Site Disaster**: Fire, short-circuits, or long-term power outages can render the Data Centre (or computer components) unusable for longer than the specified service agreement.
- **Area Disaster**: Floods, tornados (we cannot forget the recent 'Sandy' that created much of turmoil in US), hurricanes, snow storms can ruin a data center completely.
- **Regional Disaster**: Terrorist attacks, financial failures, etc. should never be under estimated.

An optimized data centre design softens various risks associated with all three of these categories. An appropriate data centre location can mitigate likely weather events, and other natural conditions that cannot be controlled or regulated. Smart data centre designs have uninterrupted power supply sources for sudden power failures. Organizations that have a plan in place to re-host applications will experience less disruption and likely lowered costs. As a part of risk assessment, IT managers must consider how unavoidable statuses can met with just as ease.

Step 2: Determining Requirements

After implementing the risks assessment phase, IT organizations need to classify their recovery requirements for the applications that are hosted. Requirements should be developed under the guiding parameters of:

- Recovery Point Objective (RPO): RPO is the maximum tolerable period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit to work to. For instance, 'quickest RPO' indicates zero tolerance for data loss. A 24 hour RPO would indicate that restoring data as of yesterday's backup is adequate, resulting in a loss of all transactions and data conducted after that time.
- Recovery Time Objective: RTO determines the maximum tolerable time for recovering the lost data and bringing the application back running like before. RTO indicates the time to restart systems, databases and applications on the server.

RPO and RTO requirements are directly proportionate to the cost of downtime. Cost of downtime can include actual loss of revenue, loss of employee productivity, loss of market goodwill and most importantly loss of reputation. If the cost of downtime is greater than the cost of Disaster Recovery Strategy, then (or any situation) strategy is always worth the cost. If the cost of acquiring and treasuring the customer is high then a vigilant DR strategy is a must have on the 'To-Do' checklist.

Step 3: Understanding DR Options

Backup to tape and Offsite Storage: Tape remains the cheapest and most used method for moving data to a secured data storage facility or even for archiving it. Following are some issues that are related to tape and which should never be given a blind eye:

- Tape format: The format compatibility between the source and the target should be taken good care of. Different generations of same technology can cause confusion too.

- Magnetic Disk drives Vs. Tapes: The approach involves data redundancy in an offsite data storage facility to magnetic disk drives or magnetic tapes. Disk backups can potentially reduce recovery time in the event of any disaster. Most backup applications can be restored to disk using compression technology; therefore, the backup image is much smaller in size than the actual data image.

Note: Virtual Tape Libraries (VTLs) are specialized storage devices (disk only or disk -to-tape) that can further automate the Disaster Recovery process.

- Synchronous Data Replication: Synchronous Data Replication ensures that every piece of data entered or changed is concurrently replicated. Although synchronous data replication is one of the most expensive off-site replication options.

Whatever the backup methodology, it is important to ensure that the operating system should have solid redundancy strategies so that the entire environment can be recreated even after the servers crash.

Step 4: Auditing Cloud Providers

Cloud providers should be willing to provide users with documentation regarding their data centre protection strategies. Location factor of the data centre is usually underestimated or ignored while introspecting Disaster Recovery Strategies. Clients should be vigilant towards exploring the range of data protection solutions offered by the provider. Most cloud space providers offer daily backup-to disk capabilities and some supplement that with periodic tape backup (e.g. Weekly or monthly) but that ignores the need to create immediate data redundancy. Off-site tape transfer facility should be checked under the DR strategy tools. On-site backups can help recovery from data corruption, and unintended data deletion, and allow quick restoration. Imperative elements that should be considered while auditing cloud providers are:

- Location
- Possible events
- Power Grid/ Communications Considerations and Contingencies
- Proximity to ‘prone-to-danger’ locations (e.g. any water body or any potential terrorist target areas like airports, seaports)
- Vendor’s DR emergencies

Step 5: Implementing and Managing Your Cloud DR Solution

As technological fluctuations will go round the world, cloud providers will likely be on the buying or selling side of the data centre acquisition or integration. Most important part lies in evaluating and selecting the right service provider with the right Disaster Recovery strategies, equally important is the step to review your DR requirements and solutions. The Disaster Recovery solutions should be well tested and trusted by the provider to ensure the promised performance as the DR solution that was appropriate last might turn out to be non-operative over time.