How to Run Disaster Recovery in the Cloud

What constitutes a disaster? It is an event that makes normal functioning of the organisation impossible which could be anything from a terrorist attack to a natural disaster such as a fire or flood or plumbing leak that destroys the main server.

Many businesses are located in a single place; meaning any catastrophe that could destroy a company’s physical property may also destroy business-critical documents and data. Restoring is a lengthy, expensive process so the catastrophe can ultimately destroy the business and result in it ceasing trading even if the company data isn’t destroyed.

Consequently it is imperative that every business constructs a workable disaster recovery plan (DRP) aka business continuity plan (BCP) aka business process contingency plan (BPCP) which is a plan that lays out in detail how an organization will deal with potential disasters. Given that a disaster is an event that means the normal functioning of the organisation is impossible, the DRP consists of the measures taken to minimize the effects of a disaster and the organization is able to maintain or quickly resume essential (mission-critical) functions. So, DRP requires business process analysis and continuity needs and should also include detail on disaster prevention.



When developing your DRP among the first things to appreciate is that the organisation (especially SMEs) is unlikely to have the resources (staff, expertise and hardware) to support your own in house DR centre. It is also unlikely to have either cash or the will to do so either.

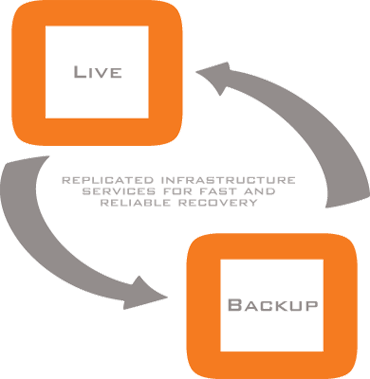
Consequently the DR plan needs to articulate how you could survive without a dedicated facility and here we look at the mechanics of doing so with data held in and/or restored from the cloud.

Developing your RTO begins by identifying and prioritizing applications, services and data, to determine the downtime that’s acceptable before a significant business impact for each. These in turn confer both the priority of the application/service plus recovery time objectives (RTOs). Taken as a whole, these create the tactics that together constitute the DRP.

Data backup is central to the DRP and how this is done plus its consequences for data restore is what creates the DRP.

The established method of backup has been to create initial backups to disk usually elsewhere in the building then write these to tape with tapes being taken off site on a daily or weekly basis. Frequently the tapes are cycled and so overwritten many times, test restores are seldom attempted and tapes have been known to go missing and the manual processes of running the backup and taking tapes off site are all too frequently forgotten. This makes for a deeply flawed process with backups at best intermittent and at worst restore can be impossible owning to the tapes themselves being unreadable (worn out) or missing. Other flaws in this process is the time to restore can run into days or even weeks and the tapes themselves are self-evidently linear so a partial restore is not possible (this may be needed when a single or small batch of documents are corrupted).

This process has been superseded by real-time or near-real-time replication and in an ideal world off-site data replication. To ensure continuity, the data replication site needs to be far enough from the main site to avoid it being overtaken by any disaster that affects the main site. The constraints here have been the bandwidth and associated costs plus occasionally distance (number of internet hops) between sites. Bandwidth issues can be mitigated by simply buying more but the DRP must be affordable and not affect the organisation’s viability.



Here we see one of the primary factors in favour of cloud based backup and disaster recovery; the “cloud” is by definition not where you are and so physically separated from your location. It is also flexible, elastic (grows and shrinks on demand), low cost, has a per use cost model and together these reasons make it attractive especially to SMEs. Dramatic falls in costs of disk storage and bandwidth together mean DR solutions previously only available to the enterprise clients are now eminently deliverable to the SME market.

These are the backup techniques available:

Managed Applications and Managed DR.

Under this approach both primary production and disaster recovery are in the cloud with both being handled by a managed service provider (MSP). This delivers all the benefits of cloud computing, by eliminating on-premises infrastructure and a usage-based cost model. The critical element here is choice of service provider and writing of service-level agreements (SLAs) with the most important element being the capacity to deliver uninterrupted service within the defined SLAs. Cloud only solutions are gaining popularity for email and some business applications, such as customer relationship management (CRM) with Salesforce.com and Workforce.com being good examples.

## Backup to and Restore from the Cloud.

This approach requires that applications and data are on-premises, with data backed up into the cloud and restored to on-premises hardware in case of disaster. In this way cloud backup substitutes for tape-based off-site backups and so is the least disruptive approach for most businesses.

The crucial aspect of cloud backup and recovery lies in ensuring you have a clear understanding of both the backup plus potential complications that may be posed by restore. Critically backup into the cloud and ensuring on-premises data and data in the cloud are in sync is straightforward; however, the challenging feature here data recovery. Bandwidth always has a limit and with potentially terabytes of data to be recovered, recovering that volume of data to meet your RTOs is the challenge. Frequently data can be restored to disks, which are sent for recovery, or an on-premise cache of recent backups may be used for local restore. An option here is to use features such as compression and data de-duplication which can make restores of data in the cloud to on-premises infrastructure viable but the viability of these is dependent on the nature of the data.

## Backup to and Restore to the Cloud.

Using this approach means data is restored to virtual machines in the cloud rather than on-premises infrastructure. This requires both cloud storage and cloud computer resources with the restore being done when a disaster is declared or on a continuous (pre-staged) basis. Pre-staged clients are computer account objects (virtual machines aka VMs here) that are created within Active Directory Domain Services (AD DS) before the operating system is installed. In turn these correlate with the physical devices that boot from the network by using Windows Deployment Services. Where aggressive RTOs are required, pre-staging recent (relatively up-to-date) DR VMs through scheduled restores is crucial and bringing up cloud VMs is a service some cloud service providers facilitate as part of their DR offering.

## Replication Using Virtual Machines in the Cloud.

To achieve the short recovery times (short RTOs) required by some applications the data movement option of choice is replication. Using this regime, replication to cloud virtual machines is used to protect both cloud and on-premises production. In this way replication is suitable for both on-premises-to-cloud-VM data protection and cloud-VM-to-cloud-VM. Such replication products are based on continuous data protection (CDP).

## New Options, Old Principles

It is a truism that the cloud enables many more options but DR fundamentals remain the same as ever; you must have a solid DRP regularly tested with users trained and prepared for any eventuality.

For more details on cloud services, where and how to buy them, please refer to:

<http://www.managedserviceexpert.com/>