A Closer Look at Cloud-based Disaster Recovery Solutions

Introduction

In the wake of the recent natural disasters that have occurred in Asia, CIOs are scrambling to ensure that their companies are prepared when disaster strikes. Most companies agree that a sudden unexpected outage can wreak major damage in terms of compromised data or lost business, yet many do not have in place adequate disaster recovery (DR) plans, equipment and infrastructure to support a rapid and effective response.

In addition, DR has traditionally been expensive and complex – comprising entire duplicate IT infrastructure at two or more different sites, in addition to all the hands-on systems and storage management that accompanies it. Requiring extensive resources and implementation time has discouraged many enterprises from investing in DR planning and processes.

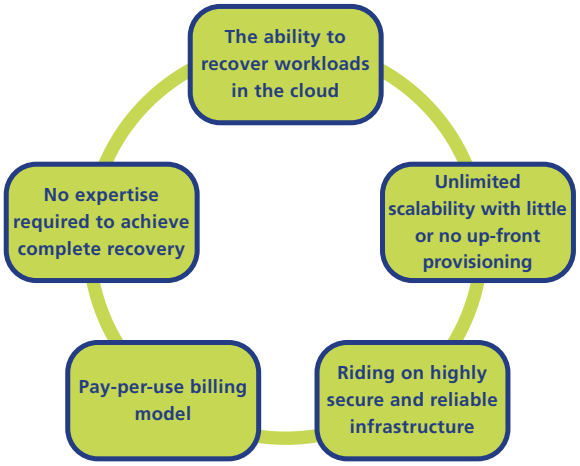
With the recent emergence of virtualization and cloud technologies, DR is now available through the cloud. Such solutions cover the whole range of eventualities, from simply duplicating data by sending files to the cloud as a form of backup to creating a private link between a customer's site and their remote dedicated cloud infrastructure including redundant, standby resources for a complete Business Continuity plan.

NTT Com Asia Enterprise Cloud Features - Issue 3

Author:
Taylor Man
Executive Vice President, New Business Division
NTT Com Asia Limited

What is a Cloud-based DR Solution?

Cloud-based DR is more versatile than simple cloud backup, and it is more efficient than remote equipment co-location. A true cloud-based DR solution possesses the following features:



The cloud can reduce the CAPEX required for traditional DR. There is no necessity to invest in a remote DR facility, and ongoing costs are lower due to the cloud being able to allocate resources and capacity on demand, thereby enabling the customer to pay only for the resources consumed. Moving DR to the cloud can also increase the flexibility of DR configurations and practices, and since clouds are designed with a view to enhancing remote management, they often fortified with highly secure and reliable infrastructure, which in turn allows for swift recovery.

To ensure that business-critical data and processes are afforded the greatest possible security and unplanned downtime is minimized, a sound cloud-based DR solution provides complete protection by allowing the customer to restore everything including IT infrastructure, data availability, and operational and business processes. The backup infrastructure is always in place and the customer can run and restore business applications in addition to reinstating data access. This minimizes downtime and quickly returns business processes to normal functioning when disaster strikes.

Backup and Recovery

One of the core aspects of DR is backup and recovery. With cloud, companies, which had been attempting to decrease the volume of duplicated data to minimize the amount that needed to be backed up, and encrypting the data on tapes for a weekly rotation, now can schedule a backup and click a button without having to be concerned with tapes while also saving system administrators' time. In addition, a sound cloud DR solution also allows incremental data backup rather than requiring the copying of complete data sets, which helps to reduce administrative load and achieve faster Recovery Time Objectives (RTOs).

In fact, the whole point of backing up is about preparing to restore data. Traditionally, companies maintained spare servers in a DR data centre, but could not avoid suffering periods of downtime while they configured new equipment when systems stalled. With cloud recovery solutions, the computing systems can run the recovered systems, and after a production system fails, companies have the ability to quickly effect a complete replacement of data and applications, and comprehensive configuration in the cloud.

Flexibility and Effectiveness

Using remote cloud infrastructure where standby applications can be configured on virtual servers and easily be turned up and down while sharing the cost of common infrastructure, service provider clouds can make DR plans more flexible. This kind of pay-as-you-go pricing model also substantially lowers the cost of "stand-by" DR.

Different levels of resources are needed before and after disaster strike. In cloud-based DR, a minimal set of resources is set aside to enable quick recovery, which can be speedily expanded in the event of an emergency. Under normal conditions, only a small amount of resources is needed to synchronize the "state" of the primary site with the cloud. Only in the case of disaster will the full amount of resources be required to run the application and hence need to be provisioned and paid for. The data and applications are mirrored between both the primary location and the cloud infrastructure, so that there are no issues in relation to recovering the original data.

The cloud creates efficiency as well. Servers can record images and take snapshots, often through an online self-service portal. If disaster occurs, the additional resources required can be brought online rapidly once any failure is detected. The fact that the virtual cloud platforms are easily automated reduces the recovery time after disaster strikes. Quick recovery time after a failure is a key component of ensuring business continuity.

Data Security and Resilience

Advanced storage technologies utilized for the purpose of building cloud-based DR are able to provide various flexible methods of securing data in order to meet a wide spectrum of user needs. If a public cloud is not preferred, there are cloud solutions available which support private clouds that use customizable configurations ranging from secure, partially partitioned hosted options to complete dedicated infrastructure implementations. This combined set of capabilities will assure organizations peace of mind and enable them to satisfy the relevant regulatory requirements in relation to their key data and applications.

It is possible to provide heightened security protocols to protect data in the cloud by employing multi-factor encryption and data segmentation, i.e. data are stored in a dedicated LUN, disk or chaises within a private network. Such features, in combination with cloud providers' multi-site, automated replication capabilities, are designed to provide maximum safeguarding of data and systems.

Closely Integrated with Existing and Remote Computers and Applications

A well designed DR solution should not force users to modify their existing application systems in order to take advantage of cloud-enabled DR. Some DR solutions allow data to be stored locally while simultaneously interfacing with cloud storage services (Storage as a Service); others provide remote private cloud storage to be built with a dedicated network and other infrastructure. This latter solution forms a private environment for directly storing data in the cloud, allowing existing infrastructure to connect to the cloud.

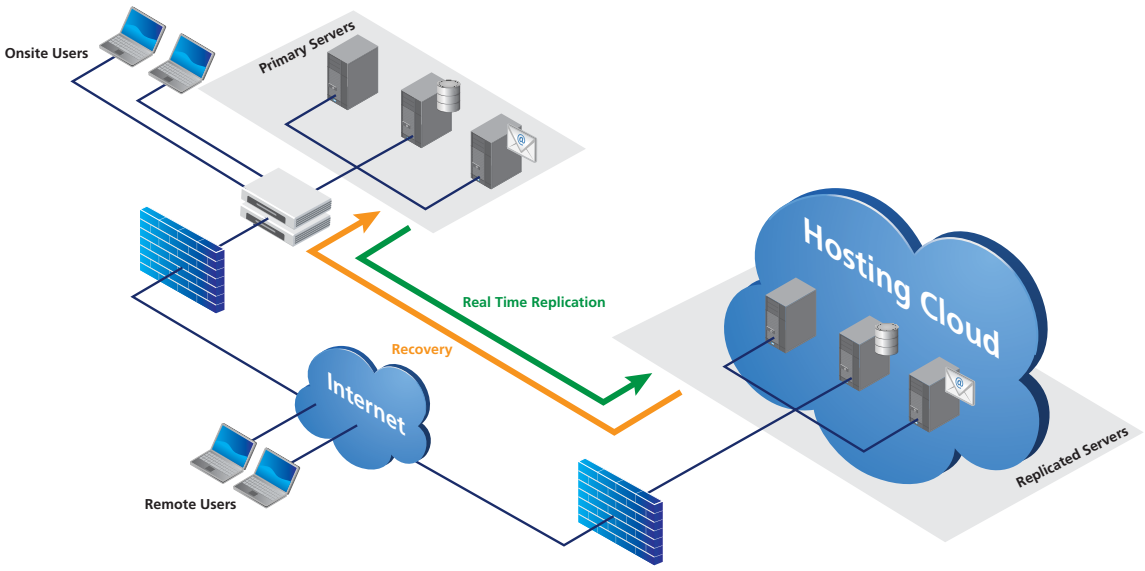
Highlights of Cloud-based DR Solutions

- Replication standby resources that mirror your primary site and are ready when you need them. You can choose multiple data protection solutions and scale them up or down to address pertinent business needs. Because they are standby, you only pay a monthly minimal fee to guarantee that the resources are available when you need them.
- Several levels of protection to help you recover from downtime. Your workload can be replicated from virtual or physical environments to the highly available cloud infrastructure and then hosted in stand-by mode. VMs can be registered in a cloud in stand-by mode— ready to be activated and keep your business up and running.
- Different data protection options to protect your business with managed backups or customized backup solutions. The managed backup solution ensures scheduled backup of data to a high-availability SANs. If your organization desires control over the backup process, Custom Backup allows you to manage the process yourself.
- Supports hybrid virtual and physical solutions – whether customers require physical servers, routers or any other particular hardware, Cloud Service Provider (CSP) is able to provide solutions to integrate these physical devices into a DR plan.

Business Resumption Centre (BRC)

Up to this point, we have addressed much of the data and systems-related DR plans and how they can be better established with cloud technology, but a complete Business Continuity Disaster Recovery (BCDR) plan must include contingencies to motivate people as well when disaster strikes. Employees need a safe place to access data, and resume operations and customer service. A service provider that can provide all-round support from cloud infrastructure and data centre facility to business resumption centre will be in a position to deliver one-stop cloud-based DR solutions to customers.

NTT Com Asia Business Resumption Centre (BRC) provides 24 x 7 x 365 facilities and services to accommodate both data and people, and is strategically located in one of the most seismically stable and secure locations in Hong Kong.



Cloud-based Disaster Recovery

NTT Com Asia BRC Attributes

BRC Services

- Dedicated & As Available
- PBX / Voice
- Email & Voicemail
- Data Vaulting & Replication
- Workstations & Servers
- Internet

Hosting Facilities

- Colocation Services
- Hosted Email / Servers / Applications services
- Networking Services
- 24 x 7 x 365 Monitored NOC
- Redundant Communication Pathways

Power

- Redundant Electric Power Grids
- Diesel Generator Backup for UPS System
- Redundant UPS System

Security

- Security IP Video Surveillance and Recording 24 x 7 x 365
- 24 x 7 x 365 Networks and Security Monitoring
- Biometric and Keycard Access Control
- Fully Locked Cabinets

In addition to the above, NTT Com Asia possesses robust cloud infrastructure and provide cloud services that assist in realizing a complete and cost efficient BCDR strategy for customers. As discussed in an earlier section, cloud-based DR provides extra benefits with regard to cost saving and flexibility as compared to traditional DR, while in the context of BRC, cloud servers and cloud desktops deliver additional value to customers with their "anywhere and anytime access" feature.

At the time a disaster strikes, employees have the option of working from any location besides the resumption centre as long as a remote device and the internet are available to access the cloud desktop. This not only helps improve RTO but also allows more or even all employees to resume work immediately, which is nearly impossible in traditional BRC environments in which only a limited number of seats can be reserved due to limited IT budgets. IT administrators now can update their OS, and maintain servers and desktops online as often as need be without having to visit the BRC physically, thus ensuring that all the systems and data are always up to date and ready for business operations.

The Ultimate Cloud DR

The movement to cloud-based DR is being supported by a broad range of CSPs and services. Each provider has its own unique technology to move DR to a cloud instead of the traditional secondary data centre. CSPs with their own data centre, network and wide range of services strategize complete DR for enterprises by, for example, deploying a secure connection to the cloud, utilizing server failover to the cloud, performing continuous data replication to the cloud and, last but not least, providing a secondary site (BRC) in order to maintain business operations. The many choices for cloud-based DR allow companies to more flexibly select a solution that integrates with their existing technology and management practices, to ultimately make DR efficient for enterprises.