Cloud-based Disaster Recovery Plan

An Overview of Cloud-based Disaster Recovery Plan

Fast-growing consumer demands have led to the evolution of innovative solutions that can drive business growth.

Along with innovative solutions arrived potential risks posing serious disaster challenges to the critical IT functioning and business continuity.

These potential risks are often referred to as man-made or natural disasters, resulting in loss of data, infrastructure failure, security breaches, among other outages.

This scenario gave rise to the concept of Disaster Recovery (DR) as a means to make an early risk assessment to avoid losses and ensure business continuity.

Disaster Recovery-as-a-Service (DRaaS) is available with various technology combinations. While there are many DR solutions available in the market, Disaster Recovery strategy powered by Cloud is considered different majorly because of ease in services and budget-friendly options.

- **Backup and Restore, Both on Cloud:** This case involves restoring of data on the cloud virtual machines rather than retrieving back to on-premise infrastructure, which requires cloud storage and cloud computing capabilities. However, the process here can be done on a continuous basis or at the occurrence of disaster. This process requires mandatory prestaging of DR Virtual Machines and keeping them updated with scheduled restores.
- **Backup to and Restore from Cloud:** This option allows you to store/backup your data onto the cloud with the on-premises infrastructure in place. At times of disasters, data gets backed up onto the cloud and restored to on-premises hardware. The real challenge is with regard to restoring, which requires relevant bandwidth speeds and network requirements to support the process. This can be addressed either by restoring data to disks making local on-premises recovery possible at the user side or using features such as compression and data dedupe, which makes data retrieval from cloud to on-premise infrastructure possible.
- **Replication:** This option is more apt for applications that demand faster recovery and maintain strong Recovery Point Objectives (RPO). Here, the data is moved in the form of replication. Replicating data to cloud VMs helps protect data both on cloud and on-premises, simply termed as 'continuous data protection' option.

Cloud-based Disaster Recovery Plan – A Snapshot

Disaster Recovery Plan (DRP) is a well-documented procedure and structured approach with checklists and implementation plans to overcome unexpected disaster recoveries:

Determining a Recovery Strategy Means Planning:

- Budgets
- Data
- Suppliers
- Management's Stance on Risks
- Management's Openness to Recovery Procedures
- Technology Availability
- Resources

Development and approval of the aforementioned recovery strategies opens ways for actual DR plan.

A basic DR Checklist involves:

- Establishing scope of the activity
- Identifying key vulnerabilities and critical assets
- Gathering relevant network infrastructure details
- Reviewing the history of past disasters and the ways they were handled
- Identifying current DR recovery strategies
- Gathering the emergency response teams
- Taking management's approval

Comprehensive Cloud Disaster Recovery Plan requires:

- Physical and virtual servers to deliver infrastructure, which can include Active Directory Servers, DNS Servers, among others
- Physical servers required to deliver applications as physical servers have a key role in delivering services and eases scaling and performance requirements
- Virtual servers needed to deliver applications, which need to be identified and created if needed considering memory, storage and virtual processor requirements
- Understanding of network configuration, which means knowing memory requirements of applications at the network layer, along with security and firewall configurations. This is critical to success of cloud DR plan

There are also some key aspects that have to be understood while opting for cloud as DR strategy. These include:

- **Bandwidth:** Given the reality that cloud functions over the network, it is mandatory to check internet and bandwidth arrangements required to redirect users to the cloud, accessibility to the network to store or retrieve data and time to restore.
- **Reliability:** It's important to check reliability of the provider in directing the users through appropriate procedures at times of disasters and in satisfying the requirements in line with the agreements made.
- **Determining Recovery Priorities:** Determining priorities as to what need to be recovered first is of high significance in dealing data recovery through cloud. This needs considering standard metrics such as Recovery Time Objective (RTO), Recovery Point Objective (RPO) and Service Level Objective (SLO). One key factor that has to be considered is the assessment of duration that might be needed to run a system on DR environment, as all disasters might not result in full loss of on-site capabilities. That varies with the type of incident, as follows:

» **Server loss:** This might involve loss of a physical or virtual server host. Failure of a virtual server host is key concern, but that might not demand movement of all applications to run in DR environment.

» **Multisystem Loss:** This case involves loss of multiple applications. Even the shared storage array might suffer an outage.

» **Data Center Loss:** This scenario might involve inaccessibility or complete loss of data center. Situations of that kind demand mandatory DR mode.

» Besides, there are also scenarios that require weeks and months' time till the recovery time. So, in such case, it has to be considered that cloud charges for the period its live recovery services are used.

▸ **Data Restore:** Cost-effectiveness apart, volumes of data to be restored in cloud from a DR scenario is also import ant to consider while dealing with cloud as a DR strategy. Its important to understand that the restoring from cloud should on a granular level, as we don't usually download gigabytes of Virtual Machine (VM) files data just for a single file. While most vendors offer this as a service, it's on firms' side to check if it is coming as a standard.

Above all, 'Security' is the key aspect that one need to think of in particular in adopting cloud as disaster recovery solution. It is important to check the way data is transferred and stored, along with a keen eye on authentication procedures, compliance requirements and encryption methods. Not just tested, they need to be ensured on paper as legal documents.

Pros and cons put in front of you. Now its time for you to decide!