Getting Started: A Guide to Disaster Recovery in the Cloud

When you hear the words hurricane or earthquake in the news, does your company's data center spring to mind? With the unfortunate disasters of recent years and the increasing reliance of business upon its technology infrastructure, it's no surprise that most IT leaders fear the impact of natural disasters on their business.

But what about the more subtle events? Local power outages. Denial of service attacks. Security breaches. System failures. Viruses. Any number of items can compromise the ability of your data center to support the business - and most won't be making the evening news.

While most companies understand the importance of a DR plan, many struggle to balance the costs with performance and risks. With cloud-based DR solutions, cost-effective business continuity options are now available to enterprises of all sizes. Use this guide as a framework to understand the information you need to get started with a DR plan that meets your needs. Understand your risks and your need, then put a plan in place.

What's at risk?

In today's digital world the question should actually be what *isn't* at risk? Whether it is an unfortunate act of nature, a technical failure or an intentional breach, unexpected disasters happen for a multitude of reasons and can cause data loss for businesses of all sizes. Without a DR solution in place you're looking at lost revenue, lost customers, diminished trust and credibility, and significant rebuilding costs.

Contact

US +1.800.697.7088
EU +44 (0) 20.7096.0149

iland.com
@ilandcloud
facebook.com/ilandcloud
youtube.com/ilandinternet

Did you know?

1. The 2012 Global Disaster Recovery Index by Acronis and the Ponemon Institute found that 86 percent of the organization respondents experienced one or more occurrences of system downtime during the previous 12 months that lasted, on average, 2.2 days.
2. Businesses calculated that the lost productivity due to the downtime cost them each more than $366,000 per year, according to the Ponemon index.
3. According to the preliminary report of a new Disaster Recovery Preparedness Council study, 72 percent of companies are not adequately prepared for an outage, whether it be caused by an act of God or human.

Getting started

While it is one of the more straightforward parts of a replication or backup plan, Disaster Recovery is not simply about backing up data in a secondary location. An effective DR plan covers end users from one environment to another in a way that allows protected data to be used in a familiar manner.

While every business is different, here are five basic steps you can take to start creating an effective DR plan.

1. Analyze your current infrastructure environment

The configuration of your IT infrastructure is an important piece of your DR plan. Examine your IT environment and have a solid understanding of what you are working with before planning a cloud-based DR implementation. Ask yourself:

- What would happen if we experienced an event today?
- Do we have the processes and staff to pull through?
- Is our plan documented, tested and updated frequently?
- How will our users react?
- What kind of storage do we currently have?
- What systems are in place?
- What is our mix of physical and virtual machines?
- Have we already tiered our applications? If not, do we need to?
- In the event of a disaster, do we need instantaneous failover or are we comfortable with some downtime? If the latter, how much downtime?

2. Determine which data and systems to back up

Now that you've completed a frank assessment of your current status, it's time to determine what applications are mission critical. What to back up varies based on company size, industry and location. With respect to moving applications to a cloud-based Disaster Recovery environment, solutions exist to back up just about anything; which data and systems you back up are entirely up to you.

Any number of items can compromise the ability of your data center to support the business - and most won't be making the evening news.

Disaster Recovery requires planning for success. Start by identifying the applications, both internal and external, with the greatest impact on the bottom line, then build your DR plans by prioritizing accordingly. The tighter the time frame, the more expensive it will be. Ask yourself:

- What's the true impact on our business from a revenue and safety perspective, if we were left without X application?

An important consideration is how end-user access and production environment usage translates to disaster recovery. For example, a company with a high percentage of web applications needs to consider their public IP utilization, DNS cutover, geographic location of end users, load balancers, and bandwidth usage goals. A company with primarily internal systems may focus more on IPsec VPN connectivity for secondary sites, terminal services, Virtual Desktops, and WAN acceleration experience rather than data being replicated.

As you identify the critical applications, approach your DR planning with the end user in mind. The data needs to be accessed in a way that your end users understand. Having your data backed up will not be a big help in quickly getting business back on track if users do not know how to work with it.

What's the true impact on our business from a revenue and safety perspective, if we were left without X application?

3. Determine your bandwidth

Bandwidth costs have decreased considerably in recent years, but your amount of bandwidth directly affects the speed, recovery time and amount of data you should store in a cloud environment. Answer these questions:

- What bandwidth do we currently have available for upload?
- What Recovery Point Objectives (RPO) do we want?
- How often will the replicated data change? The rate of change can have implications on the bandwidth needed to maintain a current back up.

It is also important to understand, with a new DR plan, the initial synching of data can take a long time, depending on volume and bandwidth availability.

4. Plan your budget

Be realistic about your budget. Many organizations start their DR discussions wanting immediate failover and recovery for everything – until they find out the true cost. Determine what you really need and what you can live without based on the available budget. A good vendor will will work with you and provide an appropriate cloud-based DR solution that fits your budget.

5. Test it out

The only surefire way to verify your DR plan works is to test it. Cloud-based DR has made testing much easier. At a minimum, conduct an annual test to ensure you are in good shape should something unexpected occur.

- Geographical diversity of its datacenter sites.
- Multiple sites so you can choose which one is right for your organization. Many vendors do not have enough sites and some do not allow you to specify where your data resides.
- A reputation for being an experienced cloud-based disaster recovery provider.
- Strong SLAs – you need to fully understand the service-level agreement and what you can expect from the disaster recovery solution.
- Solutions that address various RTO (Recovery Time Objectives) and RPO to ensure the best approach to creating a DR plan that fits your business.
- If your business operates in a highly regulated industry, such as financial services or healthcare, make sure your solution meets the requirements for recovery of compliant environments.
- The ability to leverage your existing Multi Protocol Label Switching (MPLS) or private network to connect directly to your cloud DR site.
- The ability to co-locate physical equipment and tie it into your virtual DR infrastructure.
- Technical knowledge and experience to advise and recommend the best business alternatives for you.

About iland
iland is a cloud computing company with knowledgeable and experienced cloud architects and support teams. We provide:
SLAs: Since inception our methodologies have exceeded 99.99 percent Service Level Agreements.
Flexible pricing: Our customers consume cloud resources such as CPU, RAM, disk storage, networking and bandwidth in any way that meets their needs on a pay-as-you-go model or at a reserved rate for longer terms and larger fixed resource commitments.
Flexible implementation choices: Our clients have the option to deploy on a dedicated infrastructure or in a secure multi-tenant environment.
Customer control: Our customers can operate and manage their cloud infrastructure themselves whether it is an application, backup, or recovery, all from a centralized operations control panel.
Innovative: iland has a history of innovation in cloud services and disaster recovery/business continuity.
VMware's Partner Technical Advisory Board: iland's CTO is one of only nine cloud technologists sitting on VMware's Partner Technical Advisory Board. The Board acts on recommendations from its members and feedback from customers to continually advance DR technology and reduce its costs.

iland.com