

Business Continuity and Disaster Recovery Overview

Prepared by,

Ingram Micro Cloud, META

Contents

- 1. Introduction 3
- 2. Overview of Business Continuity and Disaster Recovery (BC/DR)..... 4
 - 2.1 What is the difference between business continuity and disaster recovery?..... 4
- 3. Importance of BCDR..... 5
- 4. Options to implement BCDR - On-premise vs Cloud 6
 - 4.1 Why BCDR on premise 6
 - 4.2 Why BCDR on Cloud 6
- 5. Conclusion..... 8

1. Introduction

This guide is intended to provide an introduction to Business Continuity and Disaster Recovery (BC/DR), why it is required and what are the options available to a customer to implement it.

2. Overview of Business Continuity and Disaster Recovery (BC/DR)

These days, organizations cannot afford a single minute of downtime. Outages can result in the loss of productivity, defection of customers and impact the reputation of your business, all of which will ultimately affect revenue. Business continuity and disaster recovery (BCDR) are closely related practices that describe an organization's preparation for unanticipated events to nonstop operations.

2.1 What is the difference between business continuity and disaster recovery?

Business continuity is more proactive and generally refers to the processes and procedures an organization must implement to ensure that mission-critical functions can continue during and after a disaster.

Disaster recovery is more reactive and comprises specific steps an organization must take to resume operations following an incident. Disaster recovery actions take place after the incident, and response times can range from seconds to days.

There are similarities between business continuity and disaster recovery. They both consider various unplanned events, from cyberattacks to human error to a natural disaster. They also have a common goal of getting the business running as close to normal as possible & as quickly as possible, especially concerning mission-critical applications.

3. Importance of BCDR

As cyberthreats increase and the tolerance for downtime decreases, business continuity and disaster recovery gain importance. These practices enable an organization to get back on its feet after problems occur, reduce the risk of data loss and reputational harm, and improve operations.

Below are few reasons what you should care about BCDR

- **Downtime is really, really, expensive:** If your employees or customers lose access to business-critical applications and data, there will be a direct impact on productivity and revenue. While this sounds obvious, many organizations do not consider the actual costs of downtime.
- **Backup Alone = Not Enough!** Every business today has conducted some form of data backup. But, what happens if your backup drive gets corrupted or fails. Sending a copy of data offsite for disaster recovery should also be considered essential. Historically, this meant sending tapes to a secondary location or tape vault. As business owner, you don't want yesterday's backup technology. Backup and business continuity are not one in the same. Your business needs both – all the time.
- **Disasters actually do happen – and they most times are not natural!** Not every disaster is broadcasted on news and weather channels. Most IT downtime is a result of common, every day actions like accidental (or even intentional) data deletion, damage to computer hardware and poor security habits.
- **Business continuity impacts everybody – especially your customers!** Data is essential for all types of organizations today, so ensuring access to applications and data following a disaster is critical. Keep in mind, failure to protect your business from human error, hardware failure and/or natural disasters can be detrimental and impact every single stakeholder.

Implementing a BCDR plan will help today's CEOs sleep a little better at night.

4. Options to implement BCDR - On-premise vs Cloud

Making decisions about business continuity (BC) and disaster recovery (DR) can be very difficult. Planning, implementing and testing BCDR can take months, and result in many sleepless nights. Additionally, some companies face the added struggles of smaller budgets, fewer resources, and a mandate for agility to remain competitive. These barriers can make choosing through the disaster recovery options, from a never-ending list of vendors, an impossible task.

Before you decide on a vendor, however, you will need to determine what type of DR solution best fits your company's needs: Cloud or On Premises.

4.1 Why BCDR on premise

Traditionally business have implemented BCDR in on-premise using the concept of primary and secondary (DR) datacenter and having data/server/storage replication configured between these datacenters. Though this scenario offers some benefits such as more control over your server, data is accessible without internet access, there are several disadvantages.

Below are common disadvantages on planning and implementing BCDR in on-premise.

- Increased capital investment to build the hardware and infrastructure.
- Growth of company means increased spending on hardware and infrastructure.
- Need for space to build/store hardware.
- Additional cost of maintenance and management.
- Need for dedicated IT support.
- Data loss is more likely to occur in the case of a disaster.
- No guaranteed uptime.

4.2 Why BCDR on Cloud

Cloud computing is taking the planet by storm. Many businesses are taking advantage of this low cost and easy-to-access option. OPEX billing model and easy scalability are one the most important benefits of working in the cloud, however there are more valuable gains from cloud. The highly advantageous option is top-notch disaster recovery. Cloud computing is making the disaster recovery process easier, faster, and more cost-effective.

Hosting the DR program in the cloud has many benefits. Below are few among them:

1. **Disks, back-up tapes etc. can be eliminated** - There is no need to maintain daily back-ups using disks, tapes etc. Though this mode can be used, compared to having a DR in the cloud, it is inefficient. The data back-up can be done, even in real-time in the cloud.
2. **Mission-critical data can be kept off-site** – Since the cloud is in a remote geographical location, in the event the production center is destroyed fully or partially, data can be recovered and production restarted within agreeable timeframe. In addition to this, the cloud service provider too would have DR plans in place.
3. **Cost effective** – Since the cloud service provider charges only for the services used, the business can pick and choose what it requires, leading to immense cost reduction. Also,

costly hardware need not be duplicated since the cloud is the resource for the DR solution. In case the production site is totally destroyed, the cloud will provide all required infrastructure & network components which can be used for Disaster Recovery and Business Continuity.

4. **Easily implemented with high reliability** – Tape drives, disks, flash drives etc. may be durable, but problems may crop up when restore functions are carried out. This would be a double disaster for the business. Compared to this, restore from the cloud has reliability equal to or greater than 99%. It makes sense going with the cloud option.
5. **Scalable** - The cloud option can be easily scaled up or down depending on business requirements.
6. **Efficiency** – Since the data is stored in the cloud, large servers and associated hardware is eliminated, leading to lower capital costs. The entire IT infrastructure of the business will be 'lean and mean', yet fighting fit, to face a disaster head-on.

Benefits of Disaster Recovery using Cloud Computing make it an ideal DR solution. It is cost effective and reliable.

5. Conclusion

If you look hard enough, you will find that there are benefits and drawbacks to any solution. The key is to find the solution with the most benefits and the least amount drawbacks for your company. Based on the information above, you may decide that your business has too much money invested in on-premises solutions to make a shift to the cloud at the moment in time. Or, you may decide that the cost benefits associated with cloud are too good to pass up. Whatever you decide, it is important to understand what is available in the industry and what new, disruptive trends are emerging.

Industry experts have analyzed and determined that conventional DR solutions are slowly going away. They're often cost ineffective, given the expense of the hardware, software, and skilled engineering staff needed to run them. In contrast to traditional solutions, cloud DR services offer a cost-effective alternative to the status quo. Cloud DR, whether run by yourself or as a service (DRaaS) makes it easy to replicate data to multiple locations and get your business up and running faster in the event of an interruption.

Protecting your business in case of disaster is full of complex decisions. While establishing a DR policy and program is a common starting point for many organizations, CIOs looking to protect their mid-sized enterprise are increasingly looking to the cloud for better options than they've had in the past.

If you are interested to know more about BCDR cloud solutions, drop us an email to iaas@ingrammicrocloud.me