Type of paper: Original scientific paper
Received: 27. 4. 2022.
Accepted: 1. 6. 2022.
DOI: https://doi.org/10.18485/edtech.2022.2.2.5
UDC: 004.4:005.934.3
004.78

Disaster recovery plan in case of business interruption and data loss

Goran Bogosavljević[1]
[1]Information Technology School – ITS, Belgrade, Serbia; simo@jakovic.com
*email address: goran46521@its.edu.rs

Abstract - Today, data is generated in large quantities. We know that cloud computing is a new type of computing platform in today's world. This type of computing generates a large amount of private data in the cloud. Therefore, the need for data recovery services is growing day by day and requires the development of efficient and effective data recovery techniques. The purpose of this paper is to present the recovery techniques and help the user collect information from any backup server when the server has lost its data and is unable to provide data to the user. This paper will also discuss several cloud recovery techniques that are used to protect data and continue business operations in case of an unexpected interruption or a disaster, either a natural one or one caused by human error or deliberate action.

Keywords: (RTO), (RPO), (DRP), (CC), (DR)

I. INTRODUCTION

Cloud computing is a computing process based on the Internet, in which all the systems are interconnected and share resources among themselves. The Internet is the medium between the cloud and users. A client is connected to the server in the cloud and can store data through the Internet and can access that data from any place. This is a communication network existing in real time, in which we can start our programmes by accessing the cloud from wherever we may be. In case of a system crash or a power cut, data may be lost which may also lead to financial losses. Destruction of this system and other problems are incurred by natural disasters and human factors.

When a disaster happens, a company has to prevent data loss. Google, Amazon, Microsoft etc. are the companies that offer their services in the cloud. If a disaster happens on the client's side, the backup copy is stored in the cloud, but if a disaster takes place in the cloud, the data will be lost.

There are some disaster recovery techniques that are used to recover data and provide the continuity of business operations, should a disastrous event occur. Each organisation has to have a disaster recovery protocol and has to test it at least two times a year.

II. THE CAUSES OF DATA LOSS

The Disaster Recovery Institute International (www.drii.org) reports that 93% of companies that experienced some form of a disaster and did not have any recovery plan, closed down within a 5-year period. Besides, 50% of companies which experience the interruption of critical business activities for longer than ten days never fully recover. This piece of information is especially significant for companies that belong to the "Fortune 500" list because their business interruption costs them $96,000 per minute on average.

A. Natural Disasters

Should natural disasters occur, a large amount of data will be lost if the Disaster Recovery Plan (DRP) has not been designed. The occurrence and strength of some natural disasters, such as storms, snow, hurricanes or torrential rain, can be predicted and approximately estimated. Some perils, such as earthquakes, fire, volcanic eruptions and landslides are unpredictable and therefore may present a much bigger threat.[1]

B. Human Factor caused Disasters

Apart from natural disasters, a large number of disasters are caused by human negligence and errors. Most disasters caused by humans are deliberate, while only a few can be considered accidental. As these cannot be easily categorised, I will mention some: terrorism, bombing, cyberattacks, theft, armed attack, and biological hazards.

C. Accidents and Technological Disasters

They are caused by human factors, but the intention is what sets them apart from those previously mentioned. They are not provoked on purpose, but are the consequence of negligence regarding maintenance, or simply outside factors beyond the possibility of making an impact on them. Among such incidents are, for example, accidents associated with power cuts, building collapses, crashes, and inaccessibility of IT infrastructure.

D. Network Intrusion

When a virus attacks apps, a disaster may ensue.

E. Hacking or Malicious Code

A disaster may happen within or outside an organisation. Although a lot of effort has been made to prevent hacking, i.e. modification of data caused by malicious code, some data loss happens.

III. TRADITIONAL DISASTER RECOVERY

There have been several levels in the course of traditional disaster recovery development.[2]

A. Level 0

There is no data outside of the location, meaning that there is no disaster recovery plan or saved data. Data recovery may last for weeks and will not be successful.

B. Level 1

There is no hot site for backup data copy, meaning that the backup copy is retrieved at an outside location and not through a hot site. The process of data retrieval for which a backup copy has been made is a long one. Because a company does not have its own redundant servers, a certain amount of time is needed to locate and set up an appropriate system.

C. Level 2

Backup data is available through a hot site, meaning that organisations maintain backup copies and hot sites, which is the fastest process of recovery. If there is a hot site in case of a disaster, applications can be activated on standby servers.

IV. DISASTER RECOVERY REQUIREMENTS

When acting towards disaster recovery, requirements are defined and there are two key features relevant to the efficient service in the cloud in case of a disaster.

A. Recovery Point Objective

The maximum period of time that may lead to data loss in case of a disaster (Recovery Point Objective – (RPO)). Generally, the necessary RPO is a business decision – for some applications no data is to be lost (RPO = 0), which means that a continuous synchronous replication is necessary, while for some other applications an acceptable loss may vary between a few seconds to several hours or even days. The RPO defines how much data a company may lose if a disaster occurs. The RPO is typically determined by the modes in which a backup copy is made and kept RPO [1]:

» Weekly backups outside the location will survive the loss of data centres while losing the amount of weekly data. Producing daily backup copies outside the location is even better.

» Daily backups on the spot will survive the manufacturing facility loss which equals a daily amount of data plus replication of transactions during the recovery period after the system crash. Producing hourly backup copies on the spot is even better.

» A database clustered in a number of data centres will survive the loss of each individual data centre without losing any data.

B. Recovery Time Objective

Recovery Time Objective refers to measuring the time needed to establish business operations again after they have been discontinued because of a disaster. RTO can be minutes, hours or days. This term may refer to the time necessary to disclose and define the kind of failure and preparation of redundant servers at the backup copy location in order to start an application operation interrupted before.

V. DISASTER RECOVERY PLAN

There are mechanisms that are applied in the creation of backup copies when disaster recovery is necessary. When a backup copy is needed, certain mechanisms are used. Three models for implementation of mirroring or replicating a site are usually mentioned, and these are: hot, warm and cold backup sites. There can be three different sources of backup copy locations [5]:

» companies specialised in disaster recovery services;
» other locations owned and managed by a company;
» mutual agreement with another organisation to share facilities where data is stored in case of disaster.

A. Hot Backup Site

Its operation is very expensive. This site works with organisations that manage processes in real time.
It is an exact copy of the original site. Data loss is minimal because the data can be transferred and work can be continued without problems. In a matter of hours, Hot Backup Site can restore production to full capacity.

B. Cold Backup Site

Is the cheapest solution. It does not require a backup copy or hardware. As there is no hardware, it can start operating at minimum cost, but requires a longer time for disaster recovery. All that is needed for restoring services to users have to be purchased and delivered to the location before the recovery operation is completed.

C. Warm Backup Site

Is already equipped with hardware at the backup copy location, situated at the primary location. To implement a Warm Backup Site, the latest backup copy needs to be delivered to the primary locations.
In a world in which technology is incorporated into almost every aspect of our lives, the cloud has truly advanced such an experience. From taking over complex operational loads to carrying out disaster recovery, the cloud has made our daily operations almost easy.
Considering such a challenging task as managing disaster recovery operations, the cloud has made us think how difficult it was to perform such operations before its appearance.
If a disaster affected the primary data centre, a backup data centre had to be provided, which would imply double operations including [3]:

» creating a physical location and facilities for IT infrastructure;
» appointing a contact person and security staff for adjustment procedures;
» enhancing server capacity for storing data and adjustments to the app scaling requirements;
» providing ancillary staff for infrastructure maintenance;
» providing the Internet connection of sufficient passband for the application to start;
» network infrastructure adjustments, including firewall, load balancers, routers and switches.

This would add to increasing costs and resources that could not be managed, leaving only a data centre as an only backup copy.

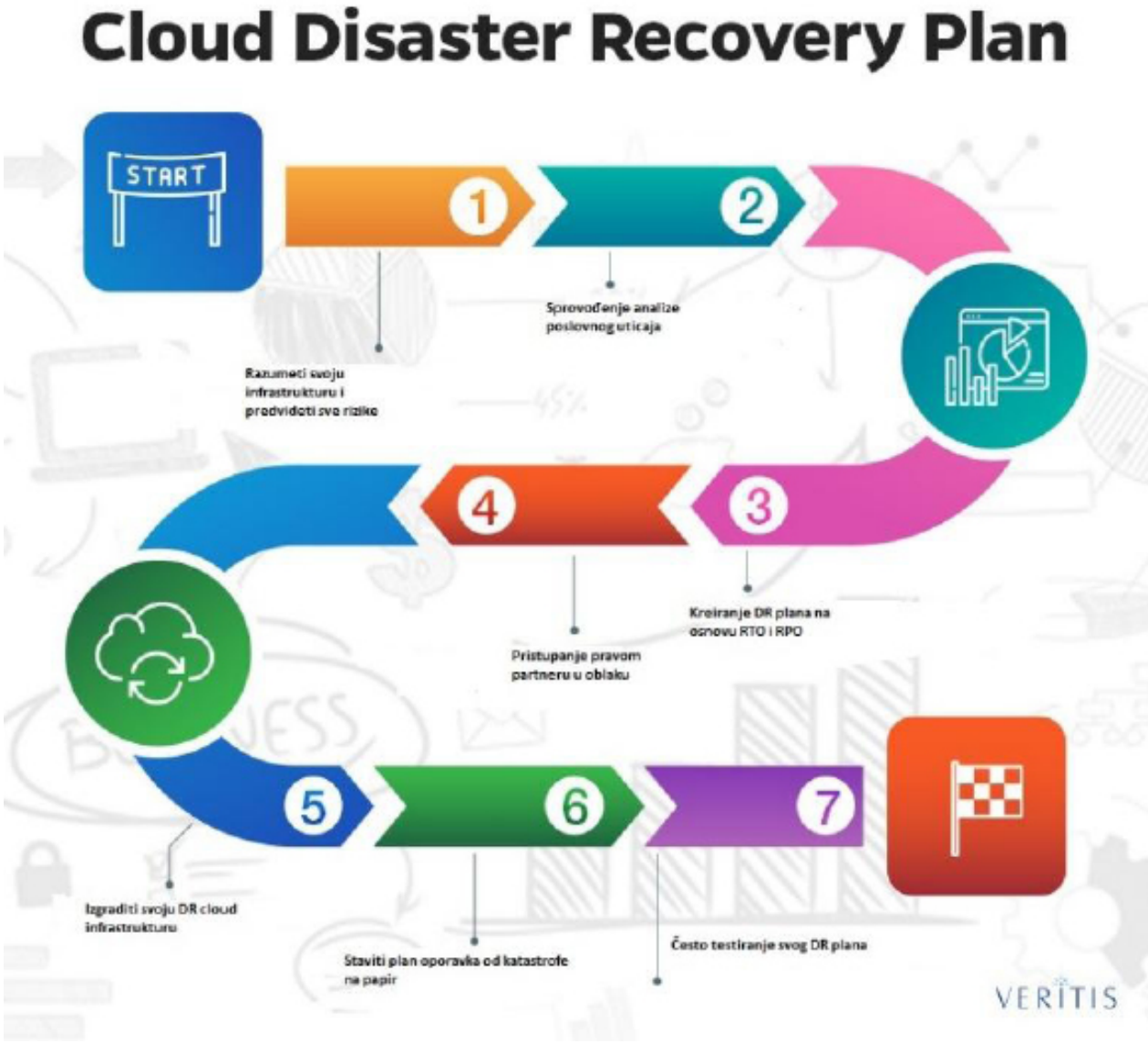

Figure 1. Steps in the Disaster Recovery Plan Creation [4].

The project Cloud Disaster Recovery offers organisations several benefits, including the following[5]:

» saving up time/capital;
» more options for backup copy locations;
» implementation simplicity with high reliability;
» flexibility.

Organisations that consider disaster recovery in the cloud for the first time and wonder where to start will find below a simple recovery plan that can help create an efficient disaster recovery strategy:

Cloud Disaster Recovery Plan – figure 1

Step 1: Understanding your own infrastructure and predicting risks

It is necessary to consider the IT infrastructure of a company, including property, equipment and data the company possesses. Also, it is necessary to establish where all these are located and how valuable they are. When the evaluation of the property is completed, risks that can affect it have to be estimated. Risks may include natural disasters, data theft, power cut etc. When the estimation is completed, the company can more efficiently design its Disaster Recovery Plan (DRP) to eliminate/minimise these risks.

Step 2: Performing a business impact analysis

A business impact analysis is the next step to do. This will enable the company to understand the limitations of its operations in case of disaster.

The following two parameters will help the company evaluate this factor:

» recovery time objective (RTO);
» recovery point objective (RPO).

The parameters relevant for data loss risk evaluation are:

a) Recovery Time Objective (RTO)

The RTO is the maximum amount of time in which a particular app can be outside the network before such an occurrence starts affecting business operations.

Scenario 1: If a company is dedicated to providing services promptly, the app failure can incur a lot of costs. The company will have to invest considerable funds in a DR plan if it wants to continue business operations in a matter of minutes.

Scenario 2: If a company operates at a moderate pace, even though a disaster affects its operations, the company can still find alternative ways for conducting its business activities. It can set its RTO to a week's time. In such a case, the company will not have to invest a lot of resources into disaster recovery funds, which in turn will save enough time for providing sufficient backup resources after a disaster. Knowing your company's RTO is very important as it corresponds to the number of resources that have to be included in the DR plan because the time lost regarding the RTO can be used for gathering backup resources.

b) Recovery Point Objective (RPO)

The RPO is the maximum amount of time in which data loss for a particular app is acceptable in case of a great crisis. The points to be considered for establishing the RPO are[1]:

» a possible data loss in case of disaster;
» a possible time span before data is compromised.

If the above-mentioned scenario 1 is considered, the RPO cannot last more than 5 minutes, as the business operations are critical and cannot afford more than such a short downtime. Regarding Scenario 2, the company may wish to create its backup copy; however, as its data is not time-sensitive, the company will not need to invest a lot in its DR plan.

Step 3: Designing a DR plan based on RPO and RTO

Once a company has defined its RPO and RTO, it can focus on designing its system which will fulfil the goals of a DR plan. To implement a DR plan, the above-listed approaches can be considered [3]:

» making a backup copy and restoring the previous condition;
» Pilot Light Approach;
» warm alert state;
» a complete replication in the cloud;
» Multi-Cloud option.

It is possible to apply the combination of these approaches in the way they benefit a company's operation best, in accordance with its particular business requirements.

Step 4: Approaching the right partner in the cloud

Upon making a decision regarding the approach, the next step should be looking for a reliable service provider in the cloud that can help with implementation. If a company plans a complete replication in the cloud, it will probably want to consider the following factors before selecting the ideal service from the cloud supplier[5]:

» reliability;
» recovery speed;
» applicability;
» simplicity of adjustment and recovery;
» flexibility;
» compliance with security rules and procedures;
» factors for evaluation of an ideal cloud provider.

All the major services in the cloud providers, including AWS, Microsoft Azure, Google Cloud and IBM, have DR options. Apart from these big companies, there are also medium and small firms that offer a high-quality disaster recovery service (DRaaS).

Step 5: Building your own Cloud DR infrastructure

Having consulted its DR in the cloud partner, a company may work with a service provider on the implementation of its own DR infrastructure design and adjustments. Based on the selected DR approach the company has made, there are several logistics aspects to be considered [2]:

» How many infrastructure components will a company need?
» What is the method of data replication in the cloud?
» What are the best methods for user authentication and access management?
» What are the safety measures the company will undertake to reduce the possible risk of disaster?

It is necessary to ensure that the company's DR strategy is in compliance with its RTO and RPO specification so the business operations can run uninterrupted.

Step 6: Presenting a disaster recovery plan as a hard copy

It is important to have standard guidelines or a diagram of the process flow with specific instructions for all parties included in the DR. Should a disaster happen, each individual has to be ready to accept his/her responsibility corresponding to his/her role in the DR process. Moreover, all the instructions, in minute detail, have to be clearly explained in a hard copy. These steps ensure the DR plan's efficiency.

Step 7: Frequent testing of the DR plan

After providing a hard copy of the DR plan, the next step is frequent testing of the plan. This helps to ensure that there are no oversights in it. As a hard copy version, the plan may seem to be a comprehensive one, but the company can realise how reliable that plan is only after it has been tested.

VI. CONCLUSION

This paper demonstrates how computing in the cloud is becoming important in our daily life. Therefore, the majority of companies are based on cloud computing. They need to be aware of disasters in the cloud. When a disaster happens, all the companies face great losses, financial but also loss of data, which is the reason why disaster recovery mechanisms are introduced.

The recent research has demonstrated the importance of having a DR plan, which is supported by the information that each dollar invested in risk mitigation, e.g. a DRP, in the long run, saves up 4 dollars for the company. Therefore, it is clear that each company that conducts its business operations in a responsible manner and cares about its reputation, should approach, and perhaps, has to approach its DRP responsibly in order to protect its most valuable assets, i.e data.

BIBLIOGRAPHY

1. Abedallah Z. A., Alwan A. A., Gulzar Y. Disaster Recovery in Cloud Computing Systems: An Overview. International Journal of Advanced Computer Science and Applications; 2020; 11(9): 702–710.
2. Fox R. & Hao W. Internet Infrastructure: Networking, Web Services, and Cloud Computing. CRC Press Taylor & Francis Group. 2018. ISBN: 978-1-1380-3991-9
3. https://cloud.google.com/architecture/dr-scenarios-planning-guide (pristupano: 8. 1. 2022)
4. https://see.asseco.com/banking-and-finance/security-other-services/infrastructure-services/disaster-recovery-as-a-service-draas-607/ (pristupano: 8. 1. 2022)
5. Jaiswal V., Sen A., Verma A. Integrated Resiliency Planning in Storage Clouds. IEEE Transactions on Network and Service Management; 2014; 11(1): 3–14.