On the Requirements for Successful Business Continuity in the Context of Disaster Recovery

Saso Nikolovski[1] and Pece Mitrevski[2]

Abstract – **This paper provides an overview of the key requirements for creating a solution that will ensure successful business continuity. At the same time, a special review is made of the parameters that have not been processed in a series of researches so far, and have an important role in the success of such solutions. During review of the indicated reference papers, the key requirements for the implementation of a successful BC plan were extracted. The analysis of DR systems and the assessment of their reliability and security, especially those placed in the cloud, will be the subject of future research to extract an optimal solution to modern challenges.**

Keywords – **Business Continuity, Disaster Recovery, RTO, RPO, Fault Tolerance, Cloud Computing**

I. Introduction

Until year 2000, considerations for having a disaster recovery plan were usually based on having backups of documents and data structures on a 3-2-1 basis, and that was sufficient (due to the fact that electronic operations had not yet been developed at that time at such a level to be crucial to the company's existence, but workloads and work operations were still based on traditional methods - paper forms, fax communication, traditional postal services, classic bank payments and transactions). But after the events of 2000 and the years that followed, it became clear that backing up by any method was not enough to maintain the operability of the companies and they were only a small part of the overall solution. Statistics on the failure rate of companies after a serious outage is alarming and it should serve as a wake-up call for professionals in the field of information, but also to the company's CEO. Therefore, in today's environment, every company whose operations are based on information technologies, must respond to the need to create Business Continuity Plan (BCP), with Disaster Recovery Plan (DRP) inside, to ensure rapid recovery in the event of an outage. Nowadays, numerous researches have been conducted on the topic of Business Continuity (BC) and Disaster Recovery (DR) to consider the possible scenarios for rapid recovery from the outage and maintenance of the operation of the services. Within the paper, a review of papers is made in which this problem is processed, both from a technical and technological aspect.

II. Business continuity

Business continuity can be considered as company's disaster (incident) response with organizational plan for recovery [1]. Basically, to clarify the operability for information technology (IT) purposes, when we talk about the sustainability of business, we mean primarily the operability of IT systems (hardware and software), as a basis of information systems. The process of company's operations maintenance or their recovery, is an organizational discipline and for that reason, when considering BC, a distinction can be made between two types of continuity:

- Uninterrupted business operations and
- Recovery operations after incident/disaster

What is important to note is that in both cases, the implementation of BC is based on a Disaster Recover strategy which in the first case should maintain continuity and in the second, to ensure recovery of the company's operation after interruption. Serious approach to such planning implies two types of ensuring continuity in the work, of which the first applies to the implementation in the planning phase, and the second applies to the parallel implementation with the construction of Data Centers (DC).

As stated in the title, the purpose of this paper is to make an overview with a brief analysis, but also and introduction to research into possible solutions to ensure a successful BC, with special emphasis on recovery solutions after an incident.

A. Uninterrupted operation continuity

In contemporary conditions, the continuity of operations can be considered from several aspects, but as crucial are the so-called fault-tolerant mechanisms set at both hardware level (hardware components redundancy) and service level (virtualization, clustering, automation, orchestration) [2][3]. In both levels, fault-tolerant brings several penalties: increase in weight and dimensions for physical systems, size of DC, power consumption, as well as cost and time to design and test the whole solution [4]. For some "recovery after incident" scenarios, full system recovery is based on a series of these mechanisms.

1) Hardware level redundancy

This way of securing from interruptions implies placing parallel components with the existing ones in order to avoid single point of failure in some part of the whole system (power supply, network card). Given that data are crucial segment in information systems, their storage and protection against loss is of highest importance. Therefore, most commonly applied mechanisms today include the use of disk arrays to create

[1] Saso Nikolovski is with the Faculty of Information and Communication Technologies – Bitola, North Macedonia, E-mail: sasnik@gmail.com

[2] Pece Mitrevski is with the Faculty of Information and Communication Technologies – Bitola, North Macedonia, E-mail: pece.mitrevski@uklo.edu.mk

978-1-6654-8500-5/22/$31.00 ©2022 IEEE

logical storage volume (Redundant Array of Independent Disks-RAID) and the use of data storage systems (Direct-Attached Storage-DAS, Network-Attached Storage-NAS, Storage Area Network-SAN) [2]. When reviewing a series of studies that deal with these protection mechanisms, one very important part is not mentioned. That is the network infrastructure with its components, active and passive. Setting up network switches in groups (stacking), grouping network routers in active / passive mode (clustering) and providing multipath in network segments, are imposed as key in ensuring network communication with fault-tolerant protection mechanisms.

2) *Service level redundancy*

When it comes to service redundancy, the emphasis is on the availability of resources offered to customers in the internal or external network. The introduction of virtualization as a platform on which modern data centers are built and including a series of automated processes and their orchestration, introduce a new way of establishing continuity in work processes [3]. These solutions are based on installation of server clusters, managed by hypervisor with common storage space trough high availability systems to ensure uninterrupted operations in data center virtualization platforms.

B. Recovery operations after incident/disaster

If in the first type of continuity maintenance there were mechanisms that have the task of not allowing interruption in the operation of the DC, the second type includes mechanisms that should provide operational return in cases when there is an outage within the DC at the data level, application level, server system level (virtual or physical), platform level or, in the most severe form, site level outage. Each of these outages has its own specifics, primarily in the method by which operational protection is performed, and consequently in the method by which their return to function will be performed. The rules and procedures prescribed in the DRP, as an integral part of the BCP, apply to operational protection at all above levels.

III. Disaster recovery

Outages of information systems can not infrequently take on catastrophic proportions, while tending to their long-term disability. In such cases, the possession of an appropriate DRP is crucial and important for the rapid return to operation of the DC and it should not be equated with fault-tolerant mechanisms whose purpose is to protect the systems in the DC from the outage of one or more components without caused an outage of the entire DC [1][5]. Because of that, in [1][5] DR is considered as a set of pre-defined procedures and policies that are designed to enable the restoration of critical business processes and systems after a disaster. This definition of DR defines two aspects, first is to cancel or minimize data loss and the second to ensure safe recovery and operation of systems despite the loss of a certain amount of data. Consequently, DR imposes a series of conditions for its implementation, whether it is implemented with traditional techniques within DC, or a solution of DR based on cloud technologies. After reviewing the conditions that have been identified as critical to the success of DR, it should be noted that in papers that deal with the conditions as requirements for implementation of the DR, do not take into account the results of the Business Impact Analysis (BIA). Results of this analyses are crucial in obtaining a clear picture of the damage that would occur between the time of outage and the time of return to operation, but also to predicting the damage of material and intangible nature that would occur post festum. These results have a direct impact in determining all the above conditions, especially the RPO and RTO, and through them on Cost of Downtime (CoD) as parameter that is not processed in detail but has a direct impact on the overall operation.

A. Disaster recovery conditions

This section will briefly review the key conditions of DR as a process for its proper planning and accordingly, proper implementation [6][7].

1) *Recovery Point Objective (RPO)*

Generally, this condition refers to the amount of data that can be lost within a period most relevant to a business, before significant harm occurs, from the point of a critical event to the most preceding backup. As noted in [6], RPO is based on business decision, but it should be noted that some application solutions and systems despite this decision still require RPO=0.

2) *Recovery Time Objective (RTO)*

This condition represents maximum acceptable delay between the interruption of service and its restoration. This objective determines what is considered an acceptable time window when service is unavailable and is defined by the organization. According to [6], RTO as a parameter does not have only one dimension that covers only the activation time of the systems, but it also includes the time of detection of the outage, preparation of the server systems, as well as reconfiguration of the active network equipment for redirection of the entire network traffic according to the new working conditions.

3) *Performance*

Performance, as one of requirements, can be described as the ability of the DR system to enable the maintenance of the performance of applications and systems in conditions of synchronous replication for their protection, but also in conditions when their recovery process is carried out [6][7]. This condition is of great importance in the process of providing replication (synchronous or asynchronous) with the DR of DC and in conditions of occurrence of outage and implementation of DR primarily due to the connection with the RTO.

4) *Consistency*

When we talk about consistency in the recovery process after an outage, we first think about the state in which the application solutions are returned to operation, but also the services within the IT structure. According to [6] and [7], consistency can be ensured by synchronous replication of an application, service, platform, or entire site. Additionally, [6] mentions consistency provided by states stored within the local storage system, which look like consistency performed from incremental backup.

5) *Geographic location*

The geographical separation of DCs on primary and backup location is extremely important in cases of natural disasters or catastrophes caused by other factors (fires). Connection of these two locations for replication and DR scenarios is traditionally performed with synchronous or asynchronous replication and is limited by the physical distance of both locations, but also by the need for instant recovery in case of outage in some business-critical applications.

B. Business impact analysis (BIA)

According to Gartner, BIA is defined as a "process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption" [9]. From what is stated in the definition, BIA quantifies the impact of the outage in the work processes, but also directly affects the RPO and RTO as key to recover company's operability, and at the same time determines the level of protection for each area of workload processes and tolerance that can be allowed during the outage (tolerance in data lose, latency).

C. Contemporary DR solutions

In modern design conditions, several DR options can usually be noticed depending on the capabilities and needs of the user and include:

- Solutions located on premises
- Hosted solutions in the cloud and
- Hybrid solutions

Solutions located on premises, are usually based on a software, hardware or integrated solution that incorporates a hardware device with an DR platform installed as Integrated Data Protection Appliance [11].

DR solutions based on cloud infrastructure or services in the cloud [12][13], can be found as backup solutions, but in recent times (in parallel with the reduction of prices for cloud services), can be found DR solutions based entirely on cloud technologies as single or multi-cloud solutions to overcome premises infrastructure outage [5][7][12].

Hybrid solutions are combination of solution located on prem (software or hardware) with special cloud tier (or as called Cloud stack) to store data (mostly backup packages) with retention lock for predefined period in retention policy.

A challenging cloud-based DR concept involves the use of edge computing where key infrastructure resources (CPU, storage) are placed closer to users to reduce service latency and network congestion that would arise during replication and recovery processes [14].

IV. Review and analysis of different approaches to disaster recovery

The technological development today and the modern dynamics of living and working, in their compositions are completely based on the responsiveness and consistency of information services provided in data centers, covered by BCP and procedures implemented in various DR systems.

DR based on fault tolerant mechanisms in the virtual environment, as an approach are considered in [2] and there are several mechanisms for overcoming outages intended for the protection of data structures. In the continuation of the text, a review and partial analysis of some of the virtualization platforms is made, by giving relative and descriptive evaluations for each of them, without stating specific values of the amount of data returned through the recovery of VM reviewed in the present case.

Considering a different approach to building DR strategies is done in [5]. This approach is completely based on a cloud DR environment, and two scenarios are considered: a single-cloud and a multi-cloud scenario. In the framework of the overview of the key parameters and conditions, several parameters are considered, including Critical Business Function-CBF, Maximum Acceptable Outage-MAO, RTO and BIA and the links and dependencies between them are given. In the conclusion, authors address the key drawbacks of such solutions which basically have a long recovery time, and thus high RTO and CoD values.

A cloud-based service solution is discussed in detail in [6], which analyzes several scenarios by comparing their costs and performance, both in cloud and on-site. What can be noticed as a disadvantage is the absence of RTO values in both scenarios, and thus the CoD. Also, no part of the text lists the amounts of data that are protected against loss in both scenarios.

In [7], a review and description of the parameters by which such solutions are evaluated is made with additional analysis of specific techniques for DR with their advantages and disadvantages. The displayed tabular reviews of the applied techniques give the final ratings for each of them (safety, redundancy, complexity, recovery time), but do not list RPOs and RTOs for specific amounts of data recovered or system volumes, which would received a clear and solid representation of each of the concluding observations, listed in tabular and textual form.

The authors in [10] make a description and establish a methodology based on BIA which additionally emphasizes the key aspects to which special attention should be paid when designing and constructing a solution for an IT DR system. With the implementation of the solution, they manage to overcome the key shortcoming in the existing infrastructure, which is down time. The results indicate a reduction of this parameter by as much as 85%. What can be noticed as a basic shortcoming is the absence of a description of the system, albeit as a basic one, in order to get a clearer idea of what kind of DR system it is. There is also a lack of value analysis for key parameters, important for such solutions (RPO, RTO and CoD), but also infrastructure data such as its size by number of systems to be protected, the size and completeness of storage systems in which data is stored, as well as the way the connection to the global network is provided, in order to maintain the continuity of the network services.

Within [12], a comparison was made between traditional DR solutions based on hot site / cold site and a solution based on DraaS. There are a few aspects that should be paid special attention when choosing DRaaS without giving recommendations in which cases such solutions are good and in which bad solution for small and medium companies. At the end of the conclusion, more like a critical dilemma, the authors leave unanswered a key question: is really using a third party to save my data an effective solution to protect myself? This issue is extremely important in modern systems, and it plays a crucial role in choosing a cloud service, as opposed to all the parameters considered before.

Table1 provides a comparative overview of presence/absence of RTO, RPO and value of protected data in the papers listed above.

TABLE I
RTO, RPO AND VALUE OF PROTECTED DATA IN PAPERS

Reference	RTO	RPO	Data Value
[2]	/	/	/
[5]	●	/	/
[6]	/	●	/
[7]	/	/	/
[10]	/	/	/
[12]	/	/	/

V. DISCUSSION AND CONCLUSION

Papers in which DR is processed as a case, usually take into account characteristics of the solution that arise directly from the conditions for its safe implementation. As we said, in a number of them reviews and analyzes of the test results were made [6][7][13], but no special reference was made to several parameters and procedures that arise or are imposed in the process of practical implementation, such as:

- The volume of infrastructure for which a DR solution is created and its impact on the key conditions of DR especially in cases when the solution is for site recovery.
- The amount of data to be protected by the proposed solution. They have a key impact on RTO, MAO, CBF and CoD, but also on network utilization and congestion. Because of this impact, the amount of data is extremely important so it is of great importance that these systems have a quality data deduplication system, which would drastically reduce the amount of data that will be stored in DR storage systems (footprint). Considering the RTO without relating it to the amount of data to which it refers simply may not be acceptable as a relevant parameter for evaluating each DR solution. Modern backup and DR systems, during the deduplication process achieve a ratio of up to 55:1 in reducing footprint [15].
- The way and format of the data in which it will be stored. Solutions that store data in encrypted form require special hardware resources for their encryption or decryption, and thus additional time to complete the recovery process.
- Inviolability of data. This means setting security parameters (policies) that will ensure the immutability of the data. Policy checks additionally add a quantity of latency in whole process.

As important segment for the uninterrupted operation of the DC, computer networks and the connections to the global network, has not been considered and analyzed in any of the papers. For this segment, no scenarios are foreseen for its outage, no analyzes have been made for its use in cases of initial, daily, and reverse replication during the recovery process of the systems. In these cases, a series of parameters will have a direct impact on latency, RTO, CoD, but also on the entire BCP. As mentioned above in the text, latency in service usage and congestion will be the goal of future research, because as such they have a direct impact on the DR solution, but also on the overall operation of the infrastructure before and after the outage. However, putting such solutions in the cloud opens a number of possibilities for creating a flexible DR system that will be able to be flexible for scale up and scale out to meet the needs and requirements of users. When considering DR scenarios, establishing an interdependence between RTO, RPO and the amount of data is extremely important for evaluating solutions.

Therefore, future research should focus on the analysis of the relationship between these parameters, which as a result should give a correct assessment of the reliability of the implemented solution.

REFERENCES

[1] M.S. Fernando, "IT Disaster Recovery System to Ensure the Business Continuity of an Organization," National Information Technology Conference (NITC), 13-15 September, 2017, Colombo, Sri Lanka.

[2] S.Anthoniraj, Dr. S.Saraswathi, M.Anandraj, "Disaster recovery planning using fault tolerant mechanism in virtualization environment", Fourth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom2012), 2012, Bangalore, India.

[3] S.C. Joshi and K.M. Sivalingam, "Fault tolerance mechanisms for virtual data center architectures", Springer Science+Business Media, 2014, New York,

[4] E.Dubrova, "Fault-Tolerant Design", KTH Royal Institute of Technology, Sweden, Springer Science+Business Media, 2013, New York.

[5] M.M. Alshammari, A.A. Alwan, A. Nordin, I.F. Al-Shaikhli, "Disaster Recovery in Single-Cloud and Multi-Cloud Environments: Issues and Challenges", (ICETAS), 2017, Salmabad, Bahrain.

[6] T. Wood, E. Cecchet, K. Ramakrishnan, P. Shenoy, J. Van Der Merwe, A. Venkataramani, "Disaster recovery as a cloud service: Economic benefits & deployment challenges", 2010, Boston.

[7] A.A. Tamimi, R. Dawood, L. Sadaqa, "Disaster Recovery Techniques in Cloud Computing", IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019, Amman, Jordan.

[8] https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/business-continuity-plan-bcp.html. Accessed: 2022-03-23.

[9] https://www.gartner.com/en/information-technology/glossary/bia-business-impact-analysis. Accessed: 2022-03-23.

[10] M.S. Fernando, "IT Disaster Recovery System to Ensure the Business Continuity of an Organization", National Information Technology Conference (NITC), 13-15 September, 2017, Colombo, Sri Lanka.

[11] https://www.delltechnologies.com/asset/pt-pt/products/data-protection/technical-support/h16033-integrated-data-protection-appliance-ds.pdf. Accessed: 2022-03-23.

[12] H.B. Rebah, H.B. Sta, "Disaster Recovery as a Service: A Disaster Recovery Plan in the Cloud for SMEs", 2016, Sousse, Tunisia.

[13] S. Shahzadi, G. Ubakanma, M. Iqbal, T. Dagiuklas, "Autonomous, Seamless and Resilience Carrier Cloud Brokerage Solution for Business Contingencies During Disaster Recovery", 2018, Exeter, UK.

[14] T. Tsubaki, R. Ishibashi, T. Kuwahara, Y. Okazaki, "Effective disaster recovery for edge computing against large-scale natural disasters", IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 2020, Las Vegas, NV, USA.

[15] https://www.delltechnologies.com/asset/en-ee/products/data-protection/technical-support/h17254-ds-integrated-data-protection-appliance-dp4400.pdf. Accessed: 2022-03-23