Data protection and recovery performance analysis of cloud-based recovery service

Saso Nikolovski[1] and Pece Mitrevski[2]

Abstract – **An analytical modeling approach is made to the MARS cloud service. The analysis is based on a real system placed in a production environment with real influences from the rest of the IT infrastructure. Based on the results obtained from the operation of the system, a model is created that enables for service system analysis through the assessment of the values of a number of parameters for certain data protection scenarios.**

Keywords – **Cloud, Data protection, Data recovery, System Dynamics, MARS, Azure, Recovery service.**

I. INTRODUCTION

In today's environment of every company whose operation is based on information technologies, there is a need to adopt a Business Continuity Plan (BCP), which includes a Disaster Recovery Plan (DRP). The adoption of these two plans is aimed at ensuring conditions and procedures for quick recovery in cases after an outage. In the event of an outage or disaster, the unavailability of systems and services owned by organizations can cause serious consequences for modern business operations, from data loss to customer dissatisfaction, which as a consequence directly affects revenue loss.

Setting up an effective system for disaster recovery that will realistically satisfy the requirements set within the framework of the recovery plan, implies the selection of solutions correctly placed and with precisely determined values of utilization in order to fully fulfil the planned minimum, i.e. maximum values of the key parameters for their valuation.

In a series of texts resulting from research in this area, attempts have been made to position complex recovery solutions by evaluating some of the key parameters [1][2][3], without taking into account other factors that have direct impact on success in the implementation of such implementations, such as the volume of the provided structure, the amount and type of data transfer, the utilization of the systems during replication, i.e. recovery, and a series of other conditions that have an impact on maintaining the planned values of the key parameters.

In contrast to such research conducted until now, we conducted our research in a real data center, from where real values of all parameters needed for designing a DR structure were taken. Contrary to previous research, we used these values as validated in practical implementation to set up a System Dynamics model through which an analysis was made of the behavior and performance of the solution for given extreme values of the considered parameters.

II. RELATED WORKS

In most of the conducted research, the emphasis is placed on the analysis of models as a strategy for assessing the performability and availability of the foreseen solutions. What can also be noticed in the objectives of the conducted research is the attention paid to the economic profitability, that is, the cost of these solutions.

In [1], Tamimi et al. in the survey provide an overview and analysis of disaster recovery techniques based on cloud-based systems. In doing so, the research emphasis is placed on the techniques and concepts by which BCDR is provided. When considering each of the concepts, they refer to several aspects for choosing a concept and technique, of which they emphasize the economic cost effectiveness of the solution, the protection of privacy, the practicality of implementation and as a most important aspect on which they based all other aspects, emphasize reliability.

Rebah and Sta, in their paper, where they are motivated by the need of companies to protect their data structures in the event of an outage in their information systems, in [4] review the role of DRP as an integral part of BCP. In their research they make a comparative study of existing solutions for disaster recovery with special reference to the comparison with scenario-based systems for disaster recovery as a service in the cloud (Disaster Recovery as a Service-DRaaS). In addition, the research work is completely focused on the analysis and evaluation of the performance obtained by using the cloud service, and they also make a special reference to the analysis of the studies made by Gartner, Forrester Consulting and Aberdeen Group on the percentage representation of these services in disaster recovery solutions. From the point of view of the possible risks faced by the users of such services, the authors refer to the study [5] made by the company LEXSI, which in its review of the research points out a total of eight main risks that the users would face, and which should keep in mind when making the decision to implement DRP in the cloud. Mendonca et al. in several of their researches, have made a serious approach to the researches of systems and services for DR, of which in [6] they give a special reference to analyzes and modeling for the assessment of Backup as a Service-BaaS.

[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

979-8-3503-1073-3/23/$31.00 ©2023 IEEE

The research is based on analytical models and outage experiments to evaluate several of the key parameters important to disaster recovery such as Recovery time objective-RTO, Recovery point objective-RPO, availability and downtime duration. In continuation of their research, in [7], Mendonca et al. conduct research in order to determine the availability of a disaster recovery solution based on the use of multiple criteria. Here, as in [6], they use DSPN networks through which they do the modeling, but here they use the so-called Multiple-Criteria decision-making (MCDM) method for evaluating and ranking the considered solutions for disaster recovery.

In practice, regarding the applicability of the methods and algorithms developed in the research, the authors have pointed out that, for the most part, such research is done in simulation conditions with the most common application of values of the key parameters obtained in an isolated environment, i.e. without influence from the environment in which they are found, and as confirmation of their applicability, their validation obtained from their practical application is needed.

III. Production Data Center

Within this section, we present a brief description of the working environment in which we set up the test virtual machine on which the research was conducted. Taking into account that the research is carried out in a real working environment with exceptional importance for the stability of the functionality of all systems in it, a separate server system has been set up as a test virtual machine that will be used to monitor the processes for its protection (backup) and recovery/restore with included backup storage placed in the cloud as a Recovery service. The Microsoft Azure cloud is used as the service provider with using Microsoft Azure Recovery Service – MARS [9] to protect single virtual machine – VM. Compared to the DR system concept discussed in [6], where BaaS is deployed in the data center, the concept under analysis in our research is entirely based on a service deployed in the cloud.

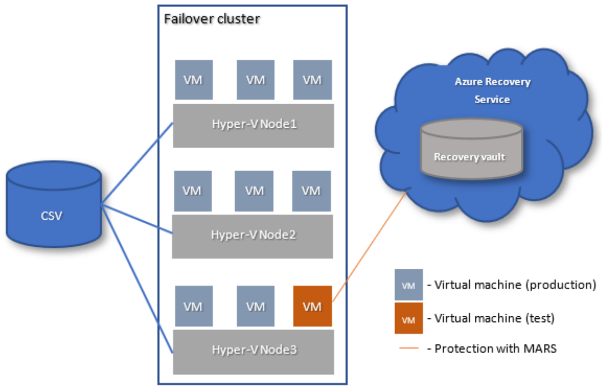


Fig. 1. Block diagram of production data center

The data center in which the research resources are placed, as a concept is shown in Fig.1 and it is production in all aspects of the organization in which it is located (information system for working with customers, electronic mail system, central control system of client systems for protection against harmful programs, central document exchange system). As can be seen from the diagram, the data center is set up on three server systems with a high degree of fault tolerance of all components in them (network and data components, power supply, internal storage systems) and a shared storage system directly connected to each of them (Direct Attached Storage-DAS) with two connection paths, where the three server systems use shared storage space (Cluster Shared Volume-CSV).

On each of the physical server systems, there is an installed server operating system Windows Server 2019 on which a virtualization platform (Hyper-V) is installed and where all three server systems as members of a virtual cluster provide a high degree of tolerance of outages (failover cluster) with which ensures high availability (HA) of the virtual systems placed in the cluster [8]. Such a concept of placement in the data center enables a high degree of availability, and thus the reliability of the services inside it and in the local network of the company where they exist.

Because it is a data center in which all the rules for ensuring the continuous operation and functionality of the systems in it are observed, during the analyzes that will be made, the availability and reliability of the data center are considered as maximum and are in accordance with the specified period of their operation. As confirmation of operation success, we have consulted security and operational records (Logs) in the systems of the data center and in service placed in the Azure platform. Regarding the service used within the Microsoft Azure cloud, the official data on its availability is close to 100%, i.e., 99.999999999% (11 nines).

A. Functionality of MARS

In the functionality part of the MARS concept, two distinctions can be made. One refers to the way of functioning when making backup copies, and the other refers to the functionality related to the recovery process. Creation backup copies of data (Fig. 2) as a process is based on the contents that will be the subject of provisioning with a backup copy through pre-defined functional scenarios.

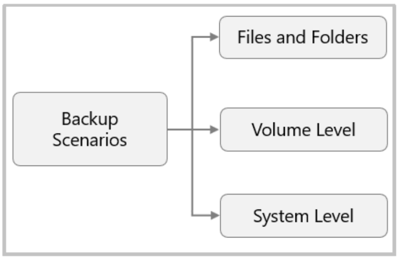


Fig. 2. Backup options in MARS concept

For research purposes, within the framework of the concept with the MARS agent, we protect the system with backups of the operational state of the system along with backups at the level of folders and files. In this way, it is possible to perform a granular (partial) repair of the target system, both from the point of view of the operation, and from the point of view of the file contents in it.

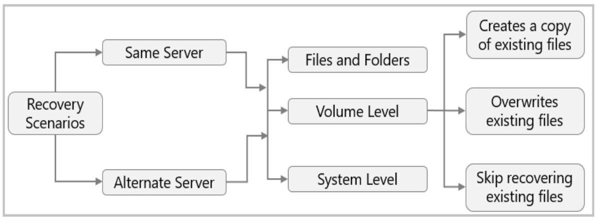

Recovery Scenarios
Same Server
Alternate Server
Files and Folders
Volume Level
System Level
Creates a copy of existing files
Overwrites existing files
Skip recovering existing files

Fig. 3. Recovery scenarios with MARS agent

From the point of view of the recovery process, the functionality of the MARS concept includes multiple scenarios, thus giving organizations and customers the opportunity to fully granular recovery of systems and data, according to their needs and goals set in the created policies for recovery from outages and disasters (Fig. 3). In all stages of preparation for implementation of the system recovery process, the RPO from which they will be put back into service is key, according to the implemented Business Impact Analysis (BIA) within the organizations BCP [10].

B. Defining values for key parameters

When defining key parameters in the analysis of the solutions covered by our research, it should be noted that they are those parameters that, from a technical point of view, have a direct impact on RPO and RTO, as two supporting parameters for evaluating the success of such solutions [9].

Considering that the analysis includes dynamic systems in which the characteristics of the parameters are constantly changing depending on the conditions under which they perform their function, it should be noted that the values of some of them are derived as average, because at the time of transfer or operation for backup/restore, the process is influenced by several factors (sporadic influences) such as delay of data packets, variable current network flow due to utilization of network connections by the rest of the infrastructure, etc.

The determination of the parameters that will be taken into account during the analysis, depends of the interest for which it is performed. The starting point from which their selection begins is the BIA, as an analysis according to which the key parameters for choosing a solution for recovery, i.e., RPO and RTO, are determined.

TABLE I
VALUES FOR KEY PARAMETERS IN BIA

Agent	Backup frequency	Retention time	RPO	RTO
MARS	daily	7 days	≤ 7 days	≤ 24 hours

According to the BIA, which is implemented as part of the protection policies in the data center, the values that are set as targets are given in Table I.

IV. MODELING AND SIMULATION

The process for creating a backup copy of the data within the MARS concept includes two steps as job1 and job2. In the first step, the agent creates a copy of the state of the virtual machine (system state), and in the second, it makes a classic copy of the data that is not covered by the first step. When setting the model as a basic model with parameter values taken directly from the MARS agent, a total of four parameters are derived: Average job1 data throughput, Average job2 data throughput, Average recovery time per MB and Total service cost per month.

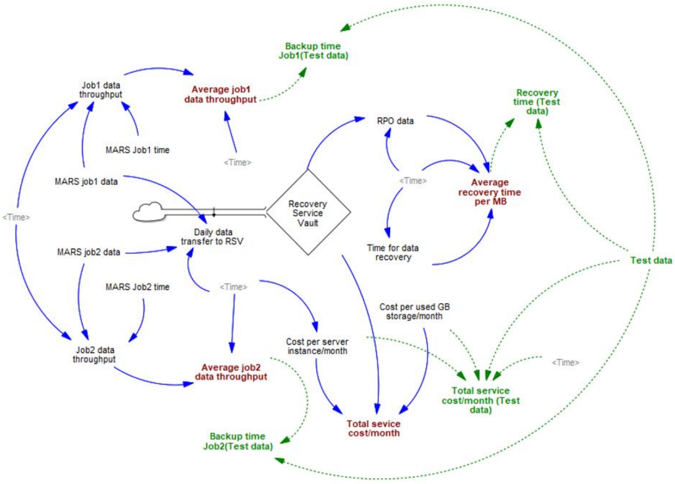

Backup time Job1(Test data)
Job1 data throughput
Average job1 data throughput
MARS Job1 time
<Time>
MARS job1 data
<Time>
Daily data transfer to RSV
Recovery Service Vault
RPO data
<Time>
Average recovery time per MB
Recovery time (Test data)
Time for data recovery
Test data
MARS job2 data
MARS Job2 time
<Time>
Cost per used GB storage/month
Cost per server instance/month
Job2 data throughput
Average job2 data throughput
<Time>
Total service cost/month (Test data)
Total sevice cost/month
Backup time Job2(Test data)

Fig. 4. Extended model of MARS concept

In addition to the time components, the model also includes the cost of using the service to get a clear estimation of the financial part of this concept, which usually has a decisive role in making the choice. Time components derived from the basic model are used to calculate the time components in the extended model, with the simulation of a given amount of test data, the values of the time components are obtained, which give a clear overview of the operation of this concept in the protection of a given structure (Fig. 4).

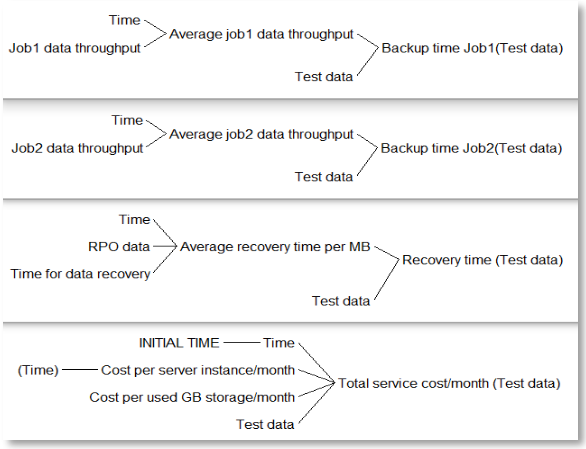
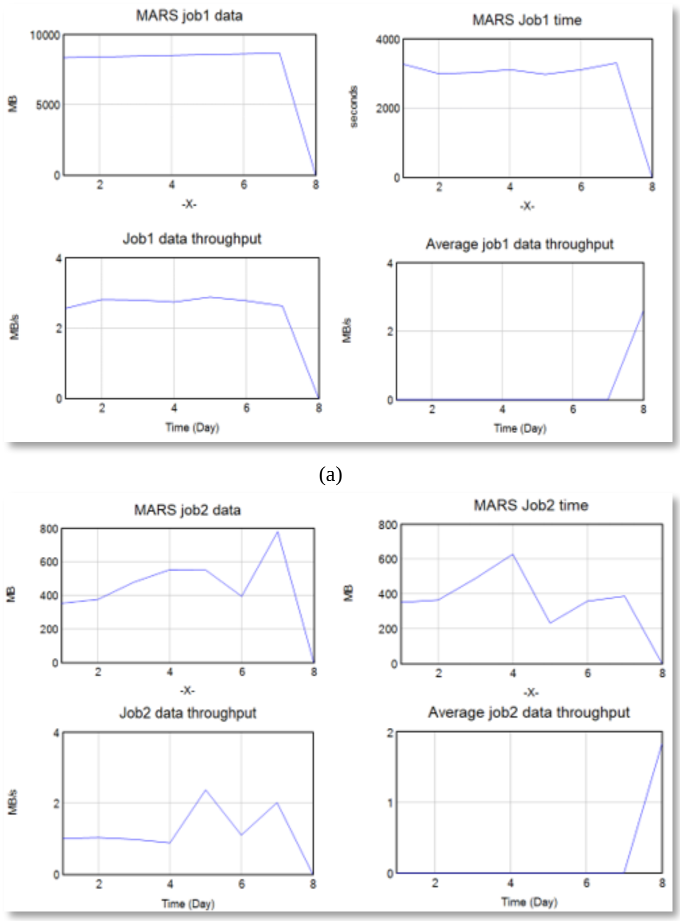

Time
Job1 data throughput
Average job1 data throughput
Backup time Job1(Test data)
Test data
Time
Job2 data throughput
Average job2 data throughput
Backup time Job2(Test data)
Test data
Time
RPO data
Time for data recovery
Average recovery time per MB
Recovery time (Test data)
Test data
INITIAL TIME
Time
(Time)
Cost per server instance/month
Cost per used GB storage/month
Test data
Total service cost/month (Test data)

Fig. 5. Causal relations between variables in extended model

As shown in Fig. 4, relationships between variables used in basic model are shown in blue color. Relations between derived variables and resulting components from extended model are shown in green color. The causal relationships between the variables in the extended model are given in Fig. 5 from where it can be noted that the components added to the basic model are consequential and have no influence on the components in the basic model.

V. Results

After performing a simulation of the system's operation with values taken from the MARS client, the graphic representation of the backup operations (job1 and job2) are given in Fig. 6a and Fig. 6b.



(a)

(b)

Fig. 6. Graphic representation of job1 (a) and job2 (b)

The average values of derived components in basic model are given in Table II.

TABLE II
VALUES FOR DERIVED COMPONENTS IN BASIC MODEL

Component	Value
Average job1 data throughput (MB/s)	2.57731
Average job2 data throughput (MB/s)	1.83045
Average recovery time per MB (sec)	5.57246

Comparing these values with values that are derived in similar solutions [6], differences are evident, because of the influences from the data center environment, as well as the influences from the network connections (both local and Internet). As a result of these influences, times to make backups and to recover data with MARS are many times greater than in [6]. But in cases where it is necessary to avoid high costs for installation of such a complex system, these results are justified.

VI. Conclusion

Within this paper, we presented part of the results of the analysis of disaster recovery systems based on cloud services. The research and analysis of the capabilities and performance of the considered system gave us results that do not meet the defined values of the parameters assigned in the BIA, in the RTO section due to the limited possibilities of transfer through the global network. Considering that this service provides satisfactory performance for systems and companies that do not require small RTO values, it can be fully applied to repair systems that allow an outage of more than one day. Systems that have a high degree of criticality for business processes in companies cannot be protected by concepts that are completely based on cloud services, but they should be protected by solutions that offer quick recovery after an outage or disaster. In such scenarios, cloud-based services can be used for long-term storage of backup copies for a specified period.

References

[1] 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.

[2] S. Shahzadi, G. Ubakanma, M. Iqbal, T. Dagiuklas, "Autonomous, Seamless and Resilience Carrier Cloud Brokerage Solution for Business Contingencies During Disaster Recovery", IEEE 20th International Conference on High Performance Computing and Communications, 2018, Exeter, UK.

[3] T. Wood, E. Cecchet, K. Ramakrishnan, P. Shenoy, J. Van Der Merwe, A. Venkataramani, "Disaster recovery as a cloud service: Economic benefits & deployment challenges", 2nd USENIX Workshop on Hot Topics in Cloud Computing, 2010, Boston.

[4] H.B.Rebah, H.B.Sta, "Disaster Recovery as a Service: A Disaster Recovery Plan in the Cloud for SMEs", Global Summit on Computer & Information Technology, 2016, Sousse, Tunisia

[5] Le secours du SI dans le Cloud, Faut-il faire le grand saut du DRaaS? Livre blanc, Lexsi, 2014.

[6] J.Mendonca, R.Lima, E.Queiroz, E.Andrade, D.S.Kim, "Evaluation of a Backup-as-a-Service Environment for Disaster Recovery", IEEE Symposium on Computers and Communications (ISCC), 2019, Barcelona, Spain.

[7] J.Mendonça, R.Lima, E.Andradey, J.Araujoy, D.S.Kim, "Multiple-criteria Evaluation of Disaster Recovery Strategies Based on Stochastic Models", 16th International Conference on the Design of Reliable Communication Networks (DRCN), IEEE, 2020.

[8] N.Dhanujati, A.S.Girsang, "Data Center-Disaster Recovery Center (DC-DRC) For High Availability IT Service", International Conference on Information Management and Technology (ICIMTech), 2018, Jakarta.

[9] B. Chakraborty, Y. Chowdhury, "Introducing Disaster Recovery with Microsoft Azure: Understanding Services and Tools for Implementing a Recovery Solution", Apress, 2020.

[10] S. Nikolovski, P. Mitrevski, “On the Requirements for Successful Business Continuity in the Context of Disaster Recovery”, Proc. of the 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), Ohrid, North Macedonia, 2022.