Mitigating Downtime with Disaster Recovery as A Service (Draas) On AWS and Azure

Upesh Kumar Rapolu

Upeshkumar.rapolu@gmail.com

Abstract

The research paper has provided about the successful application of Data Recovery As A Service which has been successful in mitigating Downtime on AWS and Azure. It has been attained by understanding the benefits, like providing the users and the development with the ability to pay for only the resources that are used. This has been curated to support complete access to the resources with a stable internet connection. As DRaaS has supported it with benefits it has also faced challenges like cyber attacks along with regulatory compliance and data security. These challenges have been limited by the utilisation of proactive strategies such as regular testing and the development of new skills. Therefore, this has been curated to determine strategic advantages in the dynamic landscapes of cloud-based disasters.

Keywords: AWS, Azure, DRaaS, Recovery Time Objective, Recovery Point Objective

I. INTRODUCTION

The following research paper will provide a nuanced understanding of mitigating downtime with disaster recovery that is meant as a service for DRaaS on AWS and Azure. DRaaS is defined as an effective service that will be responsible for minimising the chances of data loss by backing up the data and IT infrastructure within a cloud environment. At the same time, this will also be responsible for harnessing affordable storage along with minimal computing and point-in-time recovery. However, the research paper will incorporate the benefits of DRaaS on AWS and Azure and propose the challenges that are observed while implementing DRaaS. Furthermore, nurturing with efficient strategies will be used to mitigate the challenges and thus render sustainable outcomes in protecting the sensibility of the data on Azure and AWS.

II. UNDERSTANDING DraaS

The following section describes the concept of Disaster Recovery As A Service which is also abbreviated as "DRaaS". It is defined as a cloud-based platform that stands to be of paramount importance in backing up data services. At the same time, it also tends to grant the businesses to work in a streamlined manner that is rendered to control the sensitivity of the data and IT landscape in case of disaster[1]. DRaaS is also identified as a third-party service that sheds its light on resources like Recovery Time Objectives. However, the amount of evidence needed to restore the overall operations of a business is still considered to be of utmost weakness that is needed after a disaster is encountered. DRaaS functions in a mediation manner by lowering the chances of downtime errors after a disaster is committed. At the same time, this also shortens the recovery time by freeing up the IT staff to work on other projects. This makes the service accessible by the augmentation of the pay-as-you-go model and other resources such as segments like Recovery Point

Objective[2]. Thus, it is obvious that DRaaS has the power to optimise the process by replicating the data and automated recovery to combat the possibilities of errors and thus maintain ethical trust among the customers.

Figure 1: Demonstrating DraaS

III. DESCRIBING AN OVERVIEW OF CLOUD PLATFORMS

This section provides a vivid explanation of cloud platforms. Cloud platforms are defined as a virtual network of servers that is capable of supporting computing along with data storage and network services. These factors are meant for providing complete access to the internet. It is observed that cloud platforms tend to allow the users to get complete access to the resources that are needed to shed light on paying for the overall that are needed by essential resources[3]. The integration of cloud platforms is fostered in such a manner that it harnesses for utilisation to create several virtual machines in a single server. As a result, this supports the customers for running on their operating system and applications on the same physical server. Cloud platforms like AWS and Azure are considered to be beneficial for the users and the developers to grant complete access to essential data and the application from any device with a stable connection. Moreover, the segregation of cloud platforms grants full flexibility which gives the users the advantage to build cloud-native applications that make it scalable in terms of meaning the ongoing demands[4]. Furthermore, the utilisation of cloud platforms can alo be used to keep a track record of monitoring the overall health of the systems and thus nurtured with justified metrics and thus cater for the teams to respond to the issues and solve them in a mediating manner.

IV.HIGHLIGHTINGTHECHALLENGESWHILEIMPLEMENTING DraaS

The following section poses that as DRaaS comes with enormous benefits still it encounters several challenges which cannot be ignored. These challenges need to be identified at the initial stages and need to be resolved. These challenges are described below.

Cyber Attacks: It is evident that DRaaS faces challenges such as cyber-attacks under which malware along with ransomware and data breaches are seen to be observed as a significant challenge[5]. This can be harmful as it compromises data integrity followed by confidentiality and availability.

Data Security: Data security is observed as another important challenge that cannot be ignored. Catering with the data stored in the cloud the organisations must ensure that the data is protected from cyber attacks[6].

This needs robust security measures and thus considered techniques such as encryption and access to the controls.

Regulatory compliance: Another challenge is compliance. This is due to the fact that many industries are subjected to strict regulations in protecting data and privacy. Thus ensuring a cloud-based disaster helps the organisations to comply with the regulations which are determined to be critical and time-consuming.

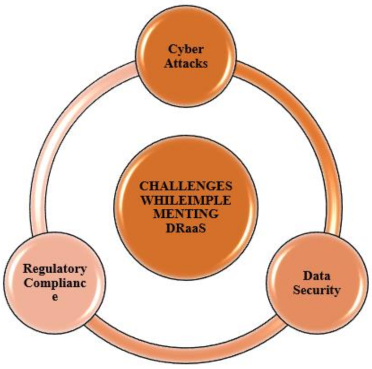

Figure 2: Depicting the Challenges While Implementing DRaaS

V. ELUCIDATINGSTRATEGIESNEEDEDFORMITIGATINGTHECHALLENGES

This section highlighted with justified challenges that are used to mitigate the issues while implementing DRaaS on AWS and Azure. These challenges are mentioned below.

Adoption to Regular Testing: This strategy is considered to be of immense vitality as it has the tendency to analyse the disaster recovery plan. As a result, this can be used to identify and address the issues before they become a problem[7].

Development of the Skills: Development of the skill is considered to be another crucial strategy that can be used to fill the skill loopholes within organisations that are invested heavily in training and development. It helps to create a bridge and thus effectively manage the organisations to manage disaster recovery.

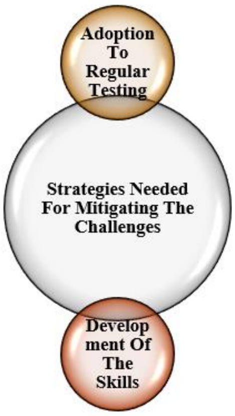
Adoption To Regular Testing
Strategies Needed For Mitigating The Challenges
Develop ment Of The Skills

Figure 3: Strategies Used to Mitigate the Challenges

IV. CONCLUSION

This research paper has explained that downtime is mitigated by Disaster Recovery As A Service on AWS and Azure in a probable manner. The benefits of DRaaS like granting both the business and the developers complete access to pay from the resources that are used only. Moreover, the challenges associated with the implementation of DRaaS which are mainly cyber attacks, data security and regulatory compliance are mitigated by the augmentation of necessary strategies which are used to resolve the issue in a proactive sense. Furthermore, the strategies used to lower challenges like regular testing and development of the skills have been used to determine justified IT infrastructure to work seamlessly within cloud-based platforms such as AWS and Azure.

Abbreviations and Acronyms

- AWS- Amazon Web Services
- DRaaS- Disaster Recovery As A Service
- Azure- Microsoft Azure
- RTO- Recovery Time Objective
- RPO- Recovery Point Objective

Units

- Recovery Time Objective (RTO) is measured in time seconds
- Recovery Point Objective (RPO) is calculated in data volumes.

Equations

- Recovery Time Objective (RTO) = [Time of Outage / Disruption - Maximum Acceptable Downtime]
- Recovery Point Objective Is calculated by measuring the time of disruption and the last backup point in which the data is usable and thus is measured in minutes.

ACKNOWLEDGEMENT

I would like to acknowledge all my professors whose constant support has helped me to complete my research paper in a given timeframe.

REFERENCES

[1] A. Baktyan and A. Zahary, “A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective,” *EAI Endorsed Transactions on Internet of Things*, vol. 4, no. 14, p. 156084, Mar. 2018.

[2] D.Shackleford, “A SANS Survey Orchestrating Security in the Cloud,” Sep. 2015.

[3] K. Shakerkhan and Ermek Tolegenovich Abilmazhinov, “Development of a Method for Choosing Cloud Computing on the Platform of Paas for Servicing the State Agencies,” *International Journal of Modern Education and Computer Science*, vol. 11, no. 9, pp. 14–25, Sep. 2019.

[4] K. Shakerkhan and Ermek Tolegenovich Abilmazhinov, “Development of a Method for Choosing Cloud Computing on the Platform of Paas for Servicing the State Agencies,” *International Journal of Modern Education and Computer Science*, vol. 11, no. 9, pp. 14–25, Sep. 2019.

[5] L. Odell, R. Wagner, and T. Weir, “Department of Defense Use of Commercial Cloud Computing Capabilities and Services,” Nov. 2015.

[6] M. Wang *et al.*, “A multi-layered performance analysis for cloud-based topic detection and tracking in Big Data applications,” *Future Generation Computer Systems*, vol. 87, pp. 580–590, Feb. 2016.