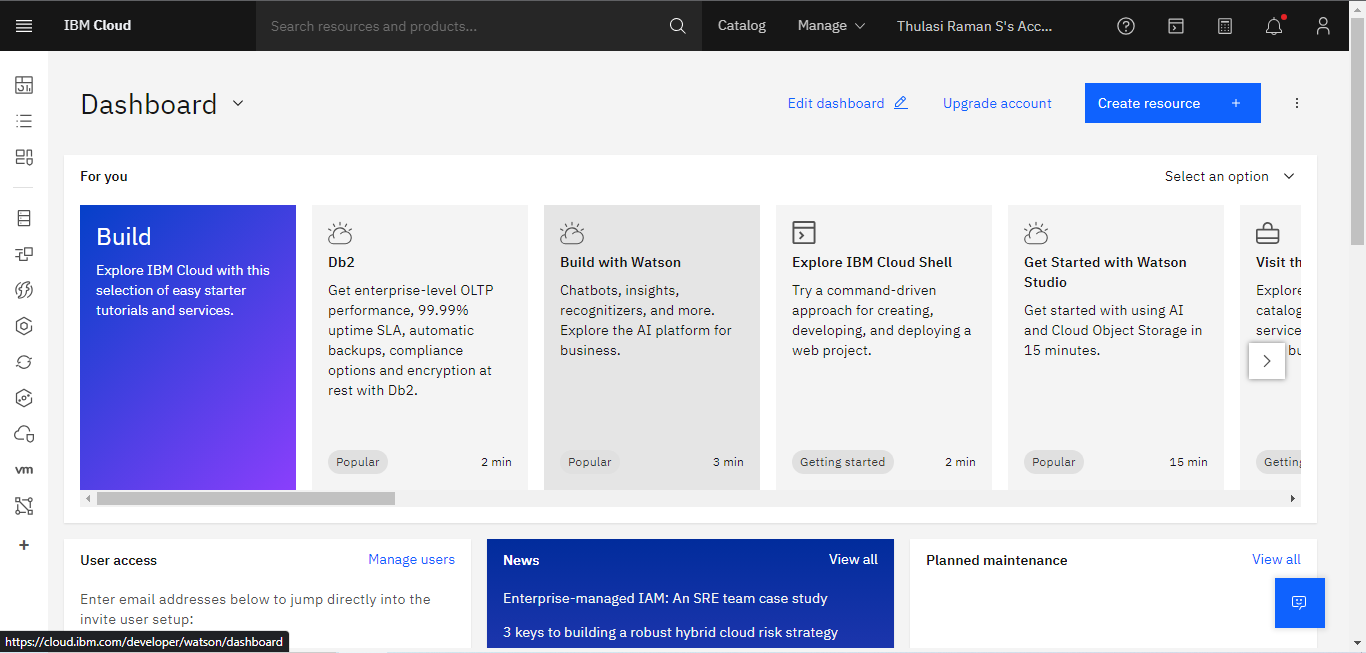
## Phase 3 :Disaster Recovery with IBM Cloud Virtual Servers

INTRODUCTION:



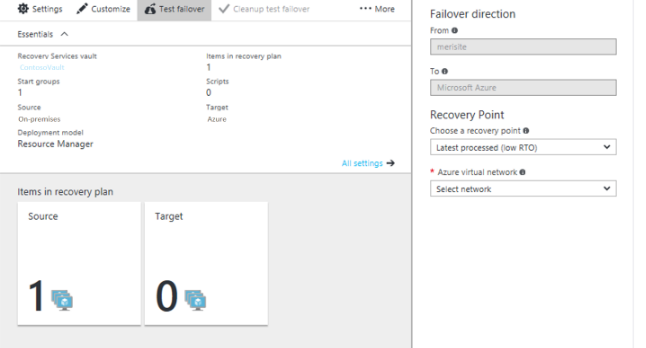
In an age where data security and uninterrupted operations are paramount, the focus on disaster recovery solutions has never been more crucial. This project aims to harness the capabilities of IBM Cloud Virtual Servers to develop a robust disaster recovery plan. By leveraging the power of virtualization and cloud-based infrastructure, we intend to create a resilient environment that ensures continuity in the event of unforeseen disasters. This project serves as a testament to the effectiveness of IBM’s cloud services in safeguarding critical data and applications.

ABOUT PHASE 3:

In this phase, we initiate the development of the disaster recovery solution using IBM Cloud Virtual Servers. We begin by setting up an IBM Cloud account and selecting the appropriate virtual server configurations. Following this, we establish a framework for disaster recovery, implementing strategies such as replication, backup, and failover mechanisms. Additionally, we perform thorough testing to validate the effectiveness of the disaster recovery plan.

DISASTER RECOVERY CONFIGURATION:

I FAILOVER TESTING



The failover testing involves simulating a disaster scenario to assess the readiness and effectiveness of the disaster recovery plan. This is typically achieved by intentionally disrupting the primary environment and activating the secondary environment to ensure seamless transition and minimal downtime. The key metrics evaluated during failover testing include recovery time objective (RTO) and recovery point objective (RPO), which determine the acceptable levels of downtime and data loss respectively.

II DATA REPLICATION

Data replication is a critical component of disaster recovery, ensuring that data is consistently mirrored from the primary environment to the secondary environment. This redundancy allows for rapid recovery in case of a failure. Different methods of replication, such as synchronous and asynchronous, can be employed based on the specific requirements and tolerances of the applications.

III BACKUP AND RESTORATION

Regular backups are essential for safeguarding data and applications. In the event of a disaster, these backups serve as a vital resource for restoration. We implement a comprehensive backup strategy, including full, incremental, and differential backups, to ensure data integrity and availability. Additionally, we establish robust procedures for testing and validating the backup and restoration processes.

IV NETWORK CONFIGURATION

The network configuration plays a crucial role in disaster recovery. It involves setting up the necessary network infrastructure to facilitate communication between the primary and secondary environments. This includes configuring virtual private networks (VPNs), subnets, and routing rules to ensure secure and efficient data transmission.

V MONITORING AND ALERTING

Continuous monitoring is essential to promptly identify any anomalies or potential issues in the disaster recovery environment. We implement monitoring tools and establish alerting mechanisms to notify relevant stakeholders in real-time. This proactive approach ensures swift action in case of any deviations from the expected state.

CONCLUSION:

The disaster recovery plan utilizing IBM Cloud Virtual Servers provides a robust framework to mitigate risks associated with unforeseen disasters. By employing failover testing, data replication, backup and restoration strategies, network configuration, and continuous monitoring, we establish a resilient environment that ensures business continuity. This project exemplifies the effectiveness of IBM’s cloud infrastructure in safeguarding critical operations.