MONTREAL COLLEGE IT

CLOUD COMPUTING CAPSTONE PROJECT 2

Prepared for: Sami Islam.

Prepared by : Cloud Computing Class

01-05-2024

Disaster Recovery Strategy for AUZA

Problem Statement:

AUZA is exposed to various disaster risks that can impact its operations and services. Currently, there is no comprehensive disaster recovery plan in place, which can lead to significant downtime, data loss, and financial impact.

Solution Overview: The project aims to develop a Disaster Recovery Strategy using cloud computing technologies to address the organization's disaster recovery challenges. The proposed solution involves using [name of cloud service provider, e.g., AWS, Azure, or Google Cloud] and implementing [disaster recovery services, tools, and approaches, e.g., backup and restore, failover, and automated recovery].

Goals and Objectives:

1. Reduce disaster recovery time objectives (RTO) and recovery point objectives (RPO) by implementing a comprehensive disaster recovery strategy using cloud computing.
2. Improve business continuity and minimize downtime by leveraging cloud-based disaster recovery services.
3. Ensure data protection and regulatory compliance by implementing backup and restore strategies in the cloud.
4. Reduce the cost and complexity of disaster recovery by utilizing cloud-based services and automation.

Justification for Cloud Computing:

1. Scalability: Cloud computing provides the ability to scale resources up or down on demand, ensuring that the organization can handle unexpected workloads during a disaster.
2. Reliability: Cloud service providers offer highly available and durable infrastructure, which can help minimize downtime during a disaster.
3. Cost-effective: Cloud-based disaster recovery services can help reduce the cost and complexity of managing on-premises disaster recovery infrastructure.
4. Automation: Cloud computing provides automation capabilities that can help streamline disaster recovery processes and minimize human error.
5. Security: Cloud service providers offer robust security features, such as encryption, access control, and monitoring, which can help protect the organization's data and services during a disaster.

Scope of Work:

1. Conduct a risk assessment to identify potential disaster scenarios and their impact.
2. Design and implement a cloud-based disaster recovery strategy, including backup and restore failover, and automated recovery.
3. Test and validate the disaster recovery strategy to ensure it meets the organization's RTO and RPO requirements.
4. Develop a disaster recovery plan and train the organization's staff on the plan.
5. Monitor and maintain the disaster recovery strategy to ensure it remains effective and up-to-date.

Deliverables:

1. Disaster recovery plan
2. Cloud-based disaster recovery infrastructure
3. Test and validation reports
4. Training materials and documentation