KGISL INSTITUTE OF TECHNOLOGY

Coimbatore – 641035

Institution code :7117

Disaster recovery with IBM cloud virtual servers

MENTOR:

MRS.INDU POORNIMA.R

TEAM MEMBERS:

DHAKSHATA.R

ANANTHI.C

ARUNA.S

HARINI.V

Disaster recovery with IBM cloud virtual servers

Objective:

The main objective for the project of implementing Disaster Recovery with IBM Cloud Virtual Servers is to ensure the continuity of critical IT services and data in the event of unforeseen disasters or disruptions.

Design Thinking:

- Identifying Critical Systems and data .
- Defining RTOs and RPOs.
- Resource Allocation for Disaster Recovery.
- Network Configuration for Disaster Recovery.
- Automation and Orchestration.
- Security and Compliance in Disaster Recovery.

Disaster Recovery Strategy :

Predictive Analytics Integration:

- Analyse historical data to identify patterns and potential disaster triggers.
- Use predictive modelling to estimate the likelihood and impact of different disaster scenarios.

Dynamic Disaster Recovery Strategy:

- Identify critical business processes and assign recovery priorities dynamically.
- Create decision trees and algorithms to guide automated responses to predicted events.

Recovery Time Objective (RTO):

RTO is the maximum allowable downtime for your systems, applications, and virtual machines in the event of a disaster. It defines the time within which these resources must be restored to normal operation to minimize the impact on your organization. To set RTO:

- Identify Critical Applications: Start by identifying the critical applications and services that your organization relies on for day-to-day operations. These are the systems that need the shortest RTO.
- Assess Tolerable Downtime: For each critical application, determine the maximum tolerable downtime. This can vary based on the application's criticality. For example, a customer-facing e-commerce platform may have a very short RTO, while a less critical internal application might have a longer RTO.
- Document RTO Values: Document the RTO values for each application or system.

Recovery Point Objective (RPO):

RPO is the maximum acceptable data loss in the event of a disaster. It defines the point in time to which data must be restored. To set RPO:

- Determine Data Criticality: Evaluate the importance of data associated with each application. For critical applications, data loss should be minimized.
- Backup Frequency: Define how frequently backups or snapshots should be taken for each application. This frequency should align with the application's data sensitivity and business requirements. For critical applications, you may need near real-time backups.
- Document RPO Values: Document the RPO values for each application.

Configure Backup and Replication Processes :

AI-Powered Automation Implementation:

- Collaborate with cloud architects to implement AI-driven automation for real-time data replication.
- Use machine learning models to optimize backup schedules and storage allocation.

Validate Recovery Procedures

Simulation and AI-Powered Testing:

- Simulate these scenarios using AI-driven testing.

- Implement AI-driven anomaly detection to identify potential issues in recovery plans.

Augmented Reality Integration:

- Use AR headsets to guide IT personnel during recovery simulations.
- Capture real-time data and performance metrics during simulations for analysis.

Testing and Validation:

- Conduct extensive testing of the entire disaster recovery solution.
- Validate the accuracy and effectiveness of predictive analytics, automation, AI-powered testing, and other components.
- Address any issues and refine the solution as needed.

Disaster recovery plan guarantees business continuity in unforeseen events:

A disaster recovery plan (DRP) is a critical component of ensuring business continuity in unforeseen events. It is a structured and documented approach to recovering IT systems and data after a disaster or disruptive event.

Risk Assessment and Preparedness:

- A robust DRP begins with a thorough risk assessment. It identifies potential risks and threats that could disrupt business operations, such as natural disasters, cyberattacks, hardware failures, or human errors.

Recovery Objectives:

- A DRP defines Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). RTO specifies the maximum acceptable downtime, while RPO determines the allowable data loss in the event of a disaster.

Redundancy and Backup:

- Disaster recovery plans include strategies for data backup and redundancy. Redundant systems and data backups are maintained offsite or in the cloud to ensure that data can be quickly restored in case of loss.

Failover Procedures:

- A well-designed DRP includes detailed failover procedures that specify how and when to switch to backup systems or data centers . This ensures that critical services can continue operating with minimal disruption.

Testing and Validation:

- Regular testing and validation exercises are integral to a DRP. These tests simulate various disaster scenarios to ensure that the plan works as intended.
- Testing identifies any weaknesses in the plan and helps improve response times and effectiveness.

Communication Plans:

- Effective communication is vital during a disaster. A DRP includes communication plans that outline how stakeholders will be informed, both internally and externally.
- Proper communication ensures that everyone knows their roles and responsibilities during a disruptive event.

GITHUB LINK: https://github.com/Dhakshata1812/Naanmudalvan.git