Disaster Recovery With IBM cloud servers

Project Team Members:

Monisha S
Ganga N
Revathy S
Sandhiya S
Viswavani H

Introduction:

Defination:

Disaster recovery (DR) consists of IT technologies and best practices designed to prevent or minimize dataloss and business disruption resulting from catastrophic events—everything from equipment failures and localized power outages to cyberattacks, civil emergencies, criminal or military attacks, and natural disasters. Many businesses—especially small- and mid-sized organizations—neglect to develop reliable, practicable disaster recovery plan. Without such a plan, they have little protection from the impact of significantly disruptive events.

Disaster Recovery (DR) is a critical aspect of IT operations to ensure business continuity in the face of unforeseen events or outages. Leveraging cloud platforms, like IBM Cloud, for DR purposes can help in efficient resource utilization, faster recovery times, and reduced overheads.
Here's a concise project overview of setting up Disaster Recovery with IBM

Design Thinking :

1. Project Objectives:

- To ensure business continuity by quickly restoring services after any form of disruption.
- Minimize data loss with a robust backup and recovery system.
- Regularly test the DR procedures to ensure they're up-to-date and functional.

2. IBM Cloud Components:

- IBM Cloud Virtual Servers: These are virtualized compute resources to run applications.
- IBM Cloud Object Storage: For storing backup data and snapshots.
- IBM Cloud Databases: Managed database services which might be part of your DR plan if you're running databases.

3. Key Steps:

1. Assessment:

- Identify critical applications and data.
- Determine the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each application.

2. Planning:

- Choose the IBM Cloud data center/region for DR.
- Determine replication mechanisms (e.g., data replication, VM snapshots).

3. Implementation:

• Set up and configure IBM Cloud Virtual Servers in the DR region.
• Implement data replication or backup solutions to IBM Cloud Object Storage
Ensure secure and efficient network connectivity between primary and DR sites.

4. Testing:
• Regularly simulate disaster scenarios to validate the recovery process.
• Document results and refine DR procedures as necessary.

5. Monitoring & Maintenance:
• Monitor DR infrastructure health and performance.
• Regularly review and update DR plans to accommodate new services or changes in the existing setup.

4. Key Considerations:

• Cost: Ensure you're optimizing costs by maybe using reserved or spot instances, depending on the DR strategy (Pilot light, warm standby, etc.).
• Security: Ensure data is encrypted at rest and in transit, and also consider network isolation for DR resources.
• Compliance: Ensure DR setup complies with relevant industry regulations or standards.

5. Benefits of Using IBM Cloud:

• Global Reach: IBM Cloud has data centers worldwide, allowing you to choose the ideal location for your DR setup.
• Integrated Services: Use services like IBM Cloud Monitoring and Logging to keep an eye on your DR infrastructure.
• Flexibility: Scale resources up or down based on requirements.

6. Challenges:

• Complexity: Setting up DR on the cloud requires in-depth knowledge of cloud services and their configurations.
• Data Transfer Costs: There might be costs associated with transferring data to/from the cloud, especially during recovery operations.

Establishing recovery time objectives, recovery point objectives, and recovery consistency objectives
By considering your risk and business impact analyses, you should be able to establish objectives for how long you'd need it to take to bring systems back up, how much data you could stand to use, and how much data corruption or deviation you could tolerate.

Your recovery time objective (RTO) is the maximum amount of time it should take to restore application or system functioning following a service disruption.Your recovery point objective (RPO) is the maximum age of the data that must be recovered in order for your business to resume regular operations. For some businesses, losing even a few minutes' worth of data can be catastrophic, while those in other industries may be able to tolerate longer windows. A recovery consistency objective (RCO) is established in the service-level agreement (SLA) for continuous data protection services. It is a metric that indicates how many inconsistent entries in business data from recovered processes or systems are tolerable in disaster recovery situations, describing business data integrity
across complex application environments.

Choosing technologies :

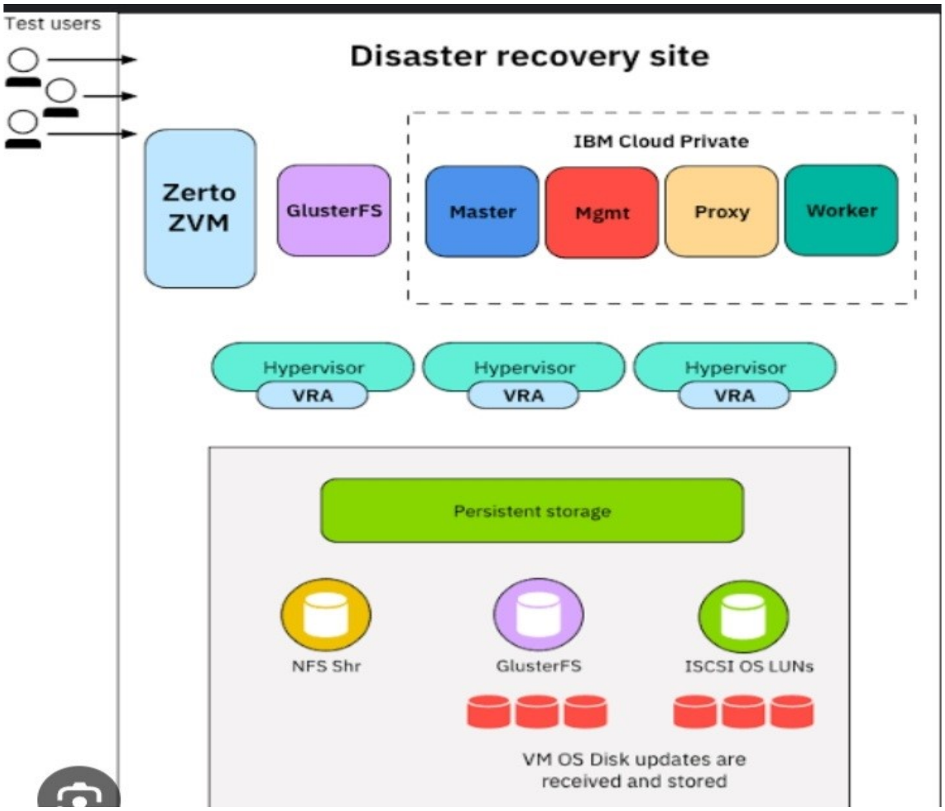
Backups serve as the foundation upon which any solid disaster recovery plan is built. In the past, most
enterprises relied on tape and spinning disks (HDD) for backups, maintaining multiple copies of their data and storing at least one at an offsite location.
In today's always-on digitally transforming world, tape backups in offsite repositories often cannot achieve the RTOs necessary to maintain business-critical operations. Architecting your own disaster recovery solution involves replicating many of the capabilities of your production environment and will require you to incur costs for support staff, administration, facilities, and infrastructure. For this reason, many organizations are turning to cloud-based backup solutions or full-scale Disaster-Recovery-as-a-Service (DRaaS) providers.

Choosing recovery site locations:

Building your own disaster recovery data center involves balancing several competing objectives. On the one hand, a copy of your data should be stored somewhere that's geographically distant enough from your headquarters or office locations that it won't be affected by the same seismic events, environmental threats, or other hazards as your main site. On the other hand, backups stored offsite always take longer to restore from than those located on-premises at the primary site, and network latency can be even greater across longer distances.

Continuous testing and review:

Simply put, if your disaster recovery plan has not been tested, it cannot be relied upon. All employees with relevant responsibilities should participate in the disaster recovery test exercise, which may include
maintaining operations from the failover site for a period of time.
If performing comprehensive disaster recovery testing is outside your budget or capabilities, you can also schedule a "tabletop exercise" walkthrough of the test procedures, though you should be aware that this kind of testing is less likely to reveal anomalies or weaknesses in your DR procedures—especially the presence of previously undiscovered application interdependencies—than a full test.



Conclusion:

As your hardware and software assets change over time, you'll want to be sure that your disaster recovery plan gets updated as well. You'll want to periodically review and revise the plan on an ongoing basis.