Disaster Recovery with IBM Cloud Virtual Servers

Phase 3

Development Part 1

Disaster recovery plan using IBM Cloud Virtual Servers

1. Identify critical systems and data that need to be protected.

2. Determine the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each system.

3. Choose the appropriate IBM Cloud Virtual Servers that meet your performance and scalability requirements.

4. Deploy redundant virtual servers in different IBM Cloud data centers or regions to ensure geographic diversity.

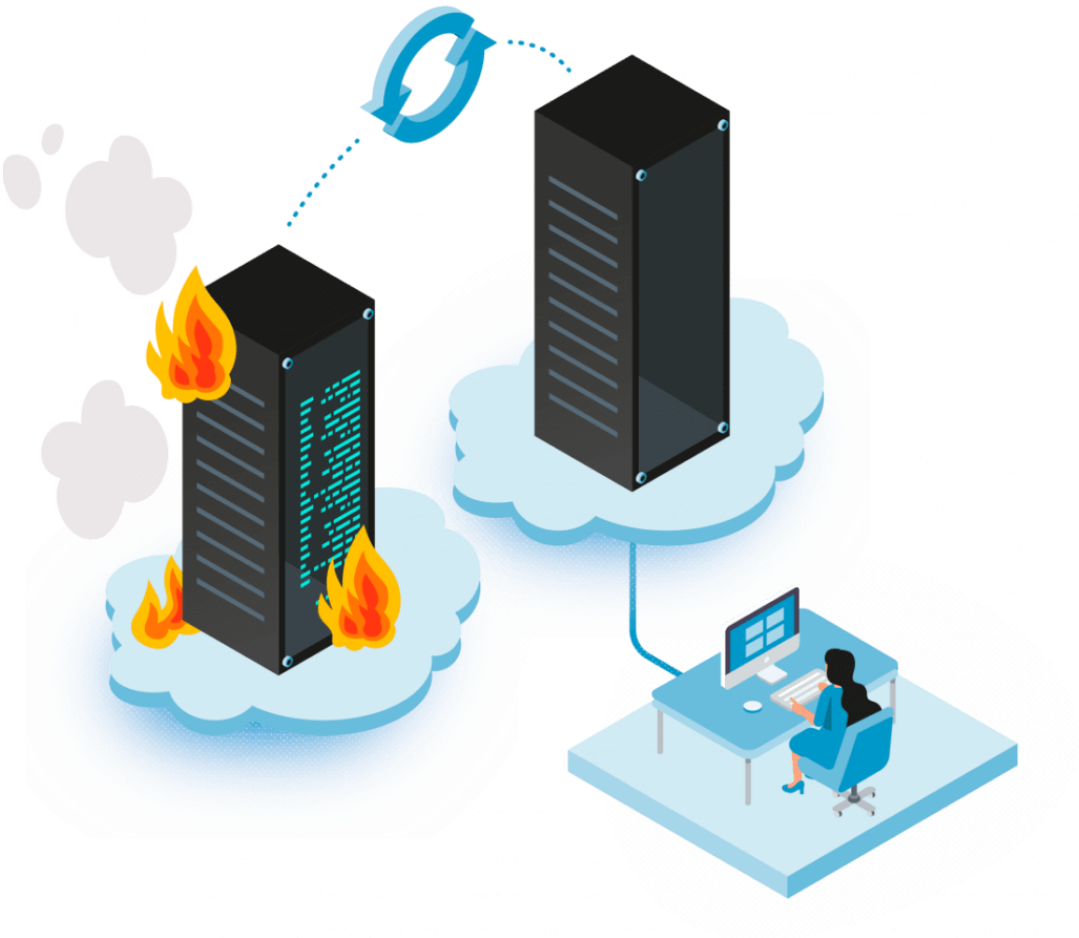
5. Use tools like IBM Cloud Object Storage or database replication to synchronize data between primary and secondary server.

6. Set up VPN or Direct Link connections between primary and secondary data centers for reliable data transformation.

7. Implement continuous monitoring to detect issues in real-time and set up alerts for critical events.
8. Develop detailed procedures for initiating failover to secondary servers and failback to primary.

9. Regularly test your disaster recovery plan to ensure it works as expected.

10. Maintain comprehensive documentation of your disaster recovery plan, including configurations, contacts, and process.



Disaster Recovery Strategy

- Data backup and restoration: You should have a comprehensive data backup plan in place to protect your organization's critical data. This plan

should include regular backups of all data, as well as offsite storage of backups to protect them from loss or damage.

- System and network redundancy: You should have redundant systems and networks in place to ensure that your business can continue to operate even if one system or network fails. This may involve using multiple data centers, cloud-based services, or other redundancy measures.

- Alternate site and equipment: You should have an alternate site and equipment that can be used to continue operations in the event that your primary site is unavailable. This site should be located in a geographically separate area to minimize the risk of being impacted by the same disaster.

- Communication and coordination: You should have a plan for communicating with employees, customers, and other stakeholders in the event of a disaster. This plan should also include procedures for coordinating the recovery effort.

- Roles and responsibilities: You should clearly define the roles and responsibilities of key personnel in the event of a disaster. This will help to ensure that everyone knows what they need to do and that the recovery effort is organized and efficient.

- Recovery Time Objective (RTO)

Define the maximum tolerable downtime for each virtual machine. This could vary depending on the criticality of the machine. For example, RTO for critical systems might be a few hours, while less critical ones could have a longer RTO.

- Recovery Point Objective (RPO)

Determine the maximum acceptable data loss in case of a disaster. For critical systems, RPO might be very low (near real-time), while for less critical systems, it could be higher (daily or even weekly backups).

- Priority of Virtual Machines

Determine the maximum acceptable data loss in case of a disaster. For critical systems, RPO might be very low (near real-time), while for less critical systems, it could be higher (daily or even weekly backups).

Regular Backups for On-Premises Virtual Machines

Choose suitable backup tools or scripts that can perform regular backups of your on-premises virtual machines. IBM

offers various backup solutions that you can integrate with your on-premises infrastructure.

Create backup schedules based on the priority of virtual machines and RPO requirements. For example, critical systems should have more frequent backups, while less critical ones can have less frequent backups.

Conclusion

By following the steps above, you can start to build a disaster recovery plan using IBM Cloud Virtual Servers. This will help you to protect your systems and data in the event of a disaster.