DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS [DEVELOPMENT (phase 3)]

1.Review and Validate Design:

Begin by revisiting the design documents from the previous phases to ensure that all requirements and specifications are clearly understood.

Verify that the design aligns with your organization's needs and goals for disaster recovery.

2.Environment Setup:

Provision the necessary IBM Cloud virtual servers and other resources as per the design specifications.

Ensure that the chosen server configurations, storage, and network settings are in place.

3.Operating System Installation:

Install the required operating systems on the virtual servers. This could include Linux or Windows, depending on your environment.

4.Software Installation:

Deploy the software and tools needed for disaster recovery, such as backup and recovery software, monitoring tools, and any custom applications identified in the design.

5.Networking Configuration:

Set up networking components to establish connectivity between the primary and backup sites. This may involve configuring firewalls, load balancers, and VPNs.

6.Data Replication and Synchronization:

Implement data replication methods to ensure that data is synchronized between the primary and secondary sites in real-time or as per the recovery point objectives (RPO) defined in your design.

7.Automation and Orchestration:

Develop automation scripts or use orchestration tools to automate the failover and failback processes.

Test the automation to ensure it works as expected in case of a disaster.

8.Testing and Validation:

Conduct thorough testing to ensure the disaster recovery solution functions as designed.

Test various failure scenarios, including server failures, network failures, and data corruption.

9.Monitoring and Alerting:

Implement monitoring and alerting systems to keep track of the health of your virtual servers and the disaster recovery solution.

Define alert thresholds and response procedures.

10.Documentation and Training:

Create comprehensive documentation that covers the setup, configuration, and operation of the disaster recovery solution.

Provide training to the relevant IT staff responsible for managing the system.

11.Security Considerations:

Implement security measures to protect sensitive data during the disaster recovery process.

Ensure that data encryption, access controls, and compliance requirements are met.

12.Compliance and Reporting:

Ensure that the disaster recovery solution complies with any industry regulations or internal policies.

Set up reporting mechanisms for auditing and compliance checks.

13.Continuous Improvement:

Establish a process for ongoing testing and maintenance to ensure that the disaster recovery solution remains effective and up to date.

14.Disaster Recovery Plan Update:

Update the disaster recovery plan with the newly implemented solution details, including any changes to RTO (Recovery Time Objective) and RPO.

15.Final Testing and Sign-Off:

Conduct a final round of testing and validation.

Seek approval and sign-off from relevant stakeholders.

16.Rollout and Transition:

Plan and execute the transition from the design phase to the operational phase, which may involve migrating workloads or data to the new disaster recovery environment.

17.Ongoing Monitoring and Maintenance:

Continuously monitor the disaster recovery environment, apply updates and patches, and make adjustments as needed to ensure its reliability.

IBM Smart Cloud Virtualized Server Recovery

IBM Smart Cloud Virtualized Server Recovery is a secure, fully managed disaster recovery solution that incorporates IBM's world-class cloud infrastructure.
The solution offers multiple business benefits to increase resiliency and help reduce the damage that IT disruptions can inflict on your company's reputation and bottom line, including:

Dramatically reduced downtime:

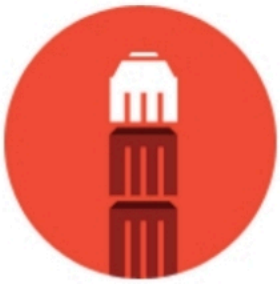
Achieve quick provisioning and short failover time with dedicated virtualised servers to reduce RTO.

Reliability:

Reduce errors and risk of data loss that can occur when recovering from unlike (heterogeneous) hardware.

Cost flexibility:

Leverage IBM's *ready-to-go* managed services to avoid the investment and time needed to build, operate and manage a resiliency solution.



Scalability:

Start with IBM Smart Cloud Virtualized Server Recovery, then work with IBM to structure comprehensive resiliency and recovery strategies for your IT infrastructure needs

Real-world success with IBM

- IBM solution helps food wholesaler reduce downtime by at least 50 percent

  A wholesale distributor in Asia Pacific was rapidly expanding its business and becoming increasingly more reliant on the quick recovery of its systems. It needed a disaster recovery solution that could reduce recovery time, as well as offer recovery services for its non-IBM systems.
  IBM Smart Cloud Virtualized Server Recovery helped this client improve its disaster recovery plan. The solution not only supported multiple server types, but, more important, helped the company cut its server recovery time by more than half—from 48 hours to 24 hours or less.

- IBM helps bank ensure business continuity affordably

  A bank in Asia needed a disaster recovery solution that could be implemented on a limited budget, yet provide comprehensive backup for its core banking applications. Bank officials also required a low recovery point objective (RPO) and low recovery time objective (RTO).
  IBM Smart Cloud Virtualized Server Recovery managed service solution helped the bank

ensure business continuity with minimal investment cost and reduced total cost of ownership. The result: the bank was able to simplify its failover process and disaster recovery drills to maintain optimal system performance. The bank also achieved a low RPO and RTO—all within budget.

Security:

- **Protecting critical data**—IBM Smart Cloud Virtualized Server Recovery is hosted within the security-rich IBM network of resiliency centre, so you can feel confident that we are protecting your sensitive data.
- **Cloud-ready data centre**—IBM has expertise and best practices gained from years of global experience managing and operating security-rich enterprise data centre.
- **Security products and services**—IBM offers a broad portfolio of security products and services to help you build cloud environments with fewer vulnerabilities, more intelligent security policies and secure information assets.

Conclusion:

This transformation process should ensure that your disaster recovery solution is not only well-implemented but also thoroughly tested and ready to protect your organization's critical data and servers in the event of disaster.