Disaster Recovery With IBM Cloud virtual Services

Phase 4: Development Part 2

Team Leader:

Tamil priyan H – 211521104166

Team Members:

Sivaraj R – 211521104148

Venkatachalam Siddhartha S – 211521104177

Ram prasad S – 211521104124

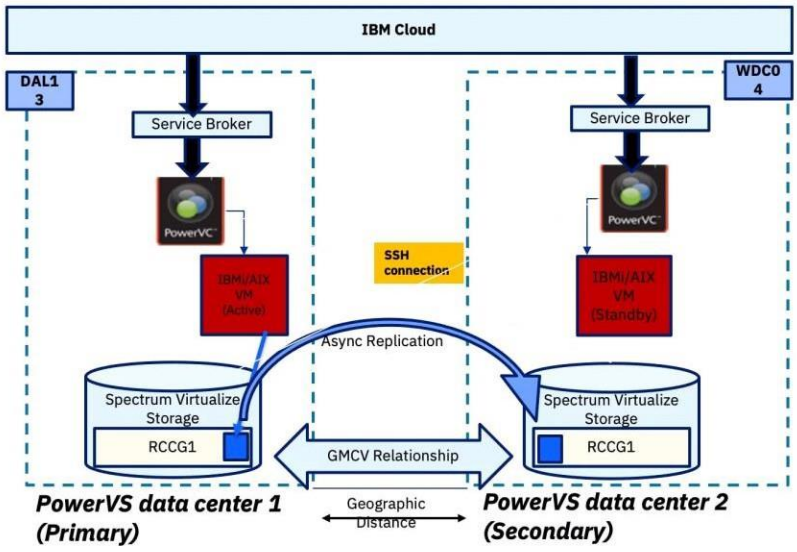
Sahaya Miheal Herson G – 211521104130

INTRODUCTION:

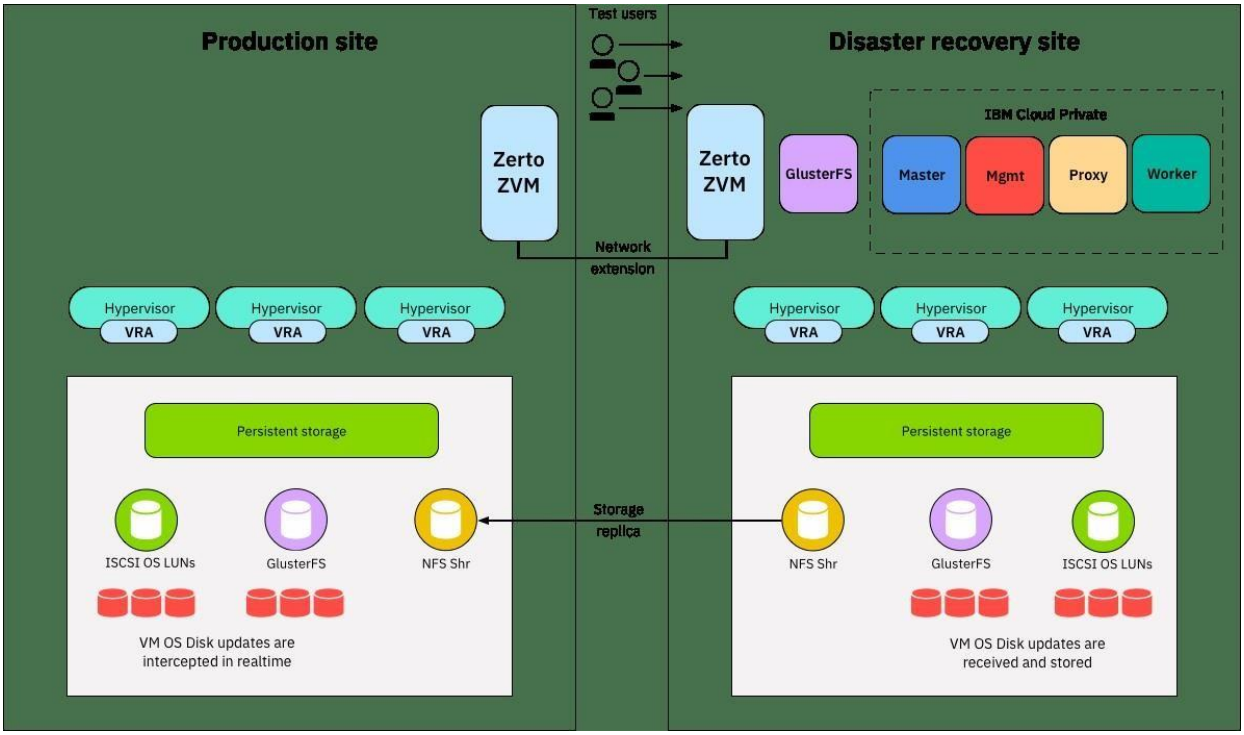
Configuring replication of data and virtual machine (VM) images from on-premises to IBM Cloud Virtual Servers is a crucial step in building a robust disaster recovery plan. Below are the steps for implementing data replication and testing recovery procedures in this context:

IMPLEMENTING DATA REPLICATION TO IBM CLOUD VIRTUAL SERVER:

1. **Choose Replication Tools:** Select a suitable replication tool or service that can efficiently transfer your data and VM images to IBM Cloud Virtual Servers. IBM offers several cloud services and tools that can assist in this process.



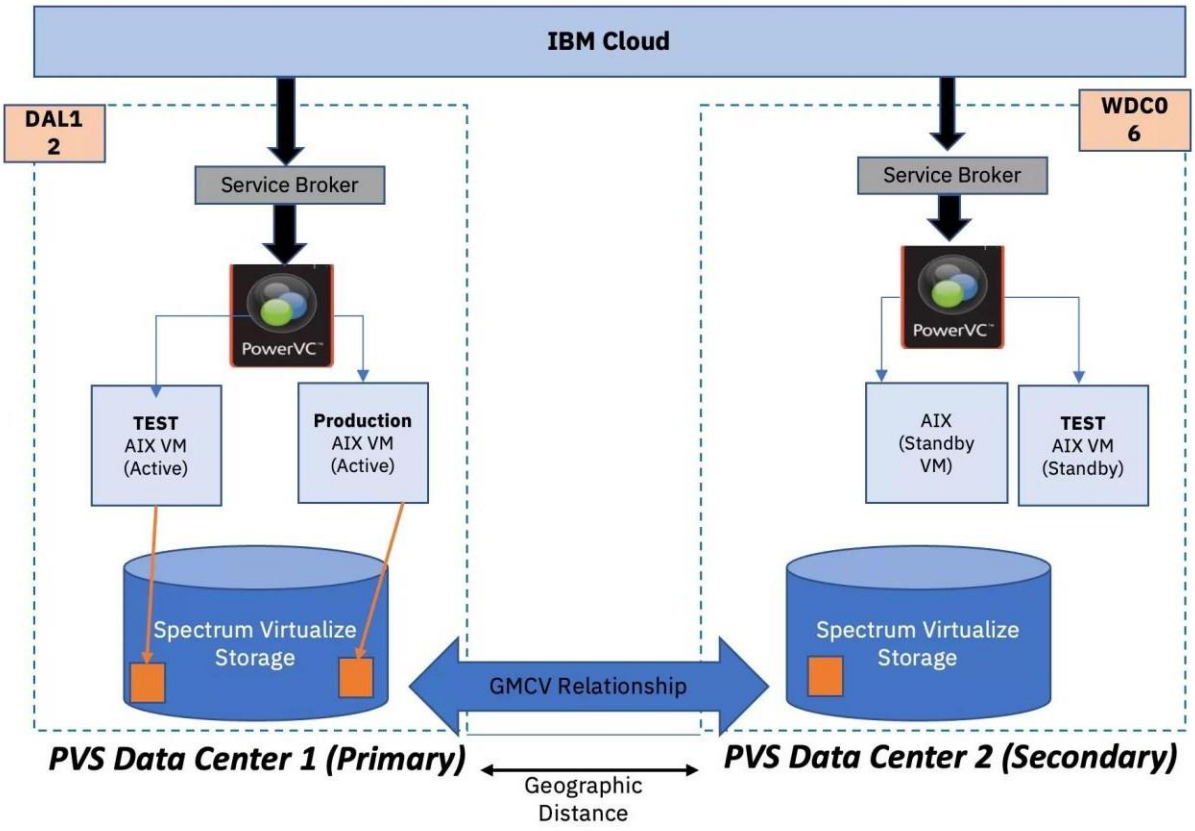
2. **Connect On-Premises and Cloud Environments:** Establish a secure network connection between your on-premises infrastructure and IBM Cloud using VPN or dedicated connectivity options.



3. **Data Backup and Replication:** Regularly back up your critical data to on-premises storage solutions. Configure replication tasks to periodically synchronize your on-premises data with IBM Cloud. This process may involve using IBM Cloud

Object Storage or block storage services to store replicated data.

4. **Replicate Virtual Machine Images:** Utilize VM image replication tools to create copies of your on-premises VMs in IBM Cloud Virtual Servers. Ensure that VM images are updated in near real-time to minimize data loss in the event of a disaster.



5. **Encryption and Security:** Encrypt data during transfer to ensure the security and privacy of sensitive information.

TESTING RECOVERY PROCEDURES:

1. **Recovery Plan Documentation:** Ensure that you have detailed documentation of your recovery plan, including step-by-step procedures for restoring data and VMs in the IBM Cloud environment.

2. **Test Scenario Definition:** Define the disaster scenario you want to simulate during the recovery test. For example, you could simulate a complete data center outage, hardware failure, or a catastrophic data loss event.

3. **Isolate Testing Environment:** Set up an isolated testing environment in IBM Cloud for the recovery test. This environment should closely resemble your production environment.

4. **Execute Recovery Procedures:** Follow the recovery procedures outlined in your documentation to restore data and VM images to the IBM Cloud environment. This should include:

    1. Restoring data from replicated backups.
    2. Spinning up VMs from the replicated VM images.
    3. Configuring network and access settings as needed.

5. **Monitoring and Verification:** Continuously monitor the recovery process to identify any issues or unexpected complications.

6. **Data Validation:** Validate the integrity of the recovered data and applications to ensure they function as expected.

7. **Failback Planning:** Develop a plan for reverting back to your on-premises environment when the disaster scenario is resolved. Test this process as well.

8. **Documentation and Reporting:** Document the results of the recovery test, including any issues encountered and lessons learned.

Revise your disaster recovery plan based on the insights gained during testing.

9. **Regular Testing:** Conduct recovery tests regularly to ensure that your disaster recovery plan remains effective and up-to-date. This testing should account for changes in your

infrastructure and applications.

CONCLUSION:

In conclusion, disaster recovery with cloud services, such as IBM Cloud Virtual Servers, involves implementing data replication for business-critical information and

thoroughly testing recovery procedures. This strategy ensures data and application availability in the face of unforeseen disasters or outages. Regular testing, documentation, and adaptation of the plan are essential for maintaining a robust and reliable disaster recovery solution that aligns with your evolving business needs and technological changes.