**Disaster Recovery with IBM Cloud Virtual Servers**

Project Documentation & Submission

* Disaster Recovery Strategy:

a. **Assessment and Risk Analysis**: Begin by assessing your organization's critical IT systems and data. Identify potential risks and vulnerabilities that could lead to disasters.

b. **Business Impact Analysis (BIA)**: Determine the impact of various disaster scenarios on your business operations, including financial, operational, and reputational consequences.

c. **Recovery Objectives**: Define recovery time objectives (RTO) and recovery point objectives (RPO) for each critical system. RTO is the maximum allowable downtime, while RPO is the maximum data loss your organization can tolerate.

d. **Resource Allocation**: Allocate necessary resources, including budget, personnel, and technology, to implement the disaster recovery plan.

e. **Plan Development**: Create a detailed disaster recovery plan that outlines specific strategies for various disaster scenarios. Ensure this plan aligns with IBM-specific technologies and tools.

* Backup Configuration:

a. **Data Classification**: Identify and classify data based on its criticality. This will help in determining the appropriate backup frequency and retention policies.

b. **Backup Tools**: Choose IBM backup solutions like IBM Spectrum Protect (formerly Tivoli Storage Manager) or other suitable products for data backup. Configure these tools to perform regular backups of critical data and systems.

c. **Backup Storage**: Ensure backups are stored securely in offsite or cloud storage locations to protect against on-premises disasters.

d. **Backup Frequency**: Define backup schedules based on RPO requirements. Critical systems might require more frequent backups.

* Replication Setup:

a. **Data Replication Technologies**: IBM offers various replication solutions, such as IBM Global Mirror for disaster recovery in storage environments. Configure data replication to maintain up-to-date copies of critical data in a secondary location.

b. **Secondary Site**: Establish a secondary site or data center where replicated data can be stored and accessed in case of a disaster.

c. **Network Connectivity**: Ensure reliable network connectivity between primary and secondary sites to support data replication.

d. **Monitoring and Failover**: Implement monitoring tools and automated failover processes to switch to the secondary site when a disaster occurs.

* Recovery Testing Procedures:

a. **Test Plan**: Develop a comprehensive testing plan that outlines the scope, objectives, and methods of disaster recovery testing.

b. **Testing Types**: Conduct various types of tests, including full-scale disaster recovery tests, partial failover tests, and data restoration tests.

c. **Regular Testing**: Schedule and perform disaster recovery tests at regular intervals to ensure the plan's effectiveness.

d. **Documentation**: Keep detailed records of test results and any issues encountered during testing. Use this information to refine and improve the disaster recovery plan.

e. **Training**: Ensure that your IT staff is well-trained on disaster recovery procedures and can execute the plan effectively during a real disaster.

It's crucial to keep your disaster recovery plan up to date as your IT environment evolves and to periodically review and adjust your backup configuration, replication setup, and testing procedures to meet your organization's changing needs and emerging IBM technologies

The "Primary Site" and "Secondary Site" are two separate locations representing your primary production data center and your secondary disaster recovery site.

Each "Server" represents individual servers in both the primary and secondary sites. The IP addresses are provided for reference.

To perform a ping test from the Primary Site to the Secondary Site, you can use the following format:



This command will send ICMP (Internet Control Message Protocol) echo requests from the primary site to the IP address of a server in the secondary site (in this case, "Server A" with IP 192.168.2.1). The response time and success of the ping requests can help you assess the network connectivity between the two sites. You can use similar ping commands for other servers in the secondary site to test their connectivity from the primary site.