DISASTER RECOVERY WITH IBM VIRTUAL SERVERS

Start building the disaster recovery plan using IBM Cloud Virtual Servers. Define the disaster recovery strategy, including RTO, RPO, and priority of virtual machines. Set up regular backups of the on-premises virtual machineusing backup tools or scripts.

Building a disaster recovery plan using IBM Cloud Virtual Servers involves several key steps, including defining your disaster recovery strategy, establishing Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and prioritizing virtual machines. Additionally, setting up regular backups of on-premises virtual machines is crucial. Here's a step-by-step guide to help you get started:

1. **Assessment and Inventory**:
    - Begin by conducting an inventory of your on-premises virtual machines, applications, and data that you need to protect.
    - Categorize and prioritize these resources based on their criticality and importance to your business operations.
2. **Define Disaster Recovery Strategy**:
    - Identify the type of disaster recovery strategy you want to implement. There are typically three main types:
        - **Cold Standby**: Minimal or no replication; manual recovery process.
        - **Warm Standby**: Periodic replication; faster recovery than cold standby.
        - **Hot Standby (Active-Active/Active-Passive)**: Continuous replication; minimaldowntime during recovery.
3. **Set RTO and RPO**:
    - Determine your Recovery Time Objective (RTO), which is the maximum tolerable downtime after a disaster. For example, if your RTO is 4 hours, your recovery process should ensure that critical systems are back up within 4 hours.
    - Establish your Recovery Point Objective (RPO), which is the acceptable data loss incase of a disaster. For instance, if your RPO is 1 hour, your data should not be morethan 1 hour old when recovered.
4. **Select IBM Cloud Virtual Servers**:
    - Choose the IBM Cloud Virtual Servers that best match your requirements, including storage, memory, and CPU resources.

- Set up the virtual servers in a geographically separate location from your on-premises infrastructure to minimize the risk of a regional disaster affecting both.

5. **Backup Strategy**:
    - Implement regular backups of your on-premises virtual machines. You can use backup tools or scripts for this purpose.
    - Ensure that backups are stored securely and are easily accessible for recovery,

6. **Replication and Synchronization**:
    - Establish a mechanism for replicating critical data and applications from your on-premises infrastructure to your IBM Cloud Virtual Servers.
    - Ensure synchronization frequency aligns with your RPO.

7. **Automation and Orchestration**:
    - Develop automation and orchestration scripts or processes to streamline the recovery procedure.
    - Test these scripts to ensure they work as expected.

8. **Testing and Validation**:
    - Regularly test your disaster recovery plan to ensure its effectiveness.
    - Perform both planned and unplanned failover drills to verify RTO and RPO targets are met.

9. **Documentation**:
    - Document your disaster recovery plan comprehensively, including step-by-step procedures, contact information, and any dependencies.

10. **Monitoring and Alerting**:
    - Set up monitoring tools and alerting systems to detect issues and anomalies in your on-premises and cloud environments.
    - Ensure that you receive timely notifications in case of any problems.

11. **Staff Training**:
    - Ensure your IT staff is well-trained and aware of their roles and responsibilities in the event of a disaster.

12. **Review and Update**:

    - Periodically review and update your disaster recovery plan to adapt to changing business needs, technology, and infrastructure.

Remember that a disaster recovery plan is a dynamic document that should evolve with your business and technological changes. It's also essential to collaborate with your cloud service provider, like IBM, to make the most of their expertise and available tools for disaster recovery.