Name : R. Shanmuga Priya

Reg No: 921821104039

Title: Disaster Recovery

Certainly, creating a disaster recovery plan using IBM Cloud Virtual Servers involves several steps. Here's a simplified guide to get you started:

Step 1: **Assess Your Infrastructure**

Identify critical applications and data that need to be backed up. Understand your network architecture and dependencies between different components.

Step 2: **Choose Backup Solutions**

Explore IBM Cloud's backup and recovery services. IBM Cloud offers solutions like IBM Cloud Object Storage and IBM Spectrum Protect Plus for data backup and recovery.

Step 3: **Design Redundancy**

Set up redundant Virtual Servers in different data centers. Use load balancers to distribute traffic and ensure high availability.

Step 4: **Implement Data Replication**

Utilize tools for real-time data replication between servers. IBM Cloud offers services like IBM Cloudant for databases and IBM Aspera for high-speed data transfer.

Step 5: **Automate Disaster Recovery**

Implement automation scripts to orchestrate failover processes. Use IBM Cloud Automation Manager to create and manage automation workflows.

Step 6: **Regular Testing**

Regularly test your disaster recovery plan to ensure its effectiveness. Simulate various disaster scenarios and evaluate the system's response.

Step 7: **Documentation and Training**

Document the entire disaster recovery process, including configurations and procedures. Ensure that your team is well-trained to handle disaster recovery situations.

Step 8: **Monitoring and Alerting**

Implement robust monitoring tools to keep an eye on your infrastructure's health. Set up alerts to notify the team in case of any anomalies.

Step 9: **Review and Update**

Regularly review your disaster recovery plan to incorporate changes in your infrastructure or technology. Stay up-to-date with IBM Cloud's latest offerings for continuous improvement.

Remember, this is a high-level overview. Depending on your specific requirements and the complexity of your infrastructure, you might need to delve deeper into each step. It's also a good practice to consult with IBM Cloud experts or follow IBM Cloud's official documentation for detailed guidance tailored to your needs.

Disaster recovery strategy refers to a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. In this context:

1. **RTO (Recovery Time Objective)**: RTO represents the targeted duration of time within which a business process must be restored after a disaster to avoid significant impact on the business. It indicates the maximum acceptable downtime for a system or process. Shorter RTOs typically require more robust and often more expensive recovery solutions.

2. **RPO (Recovery Point Objective)**: RPO defines the acceptable amount of data loss measured in time. It represents the point in time to which systems and data must be recovered after an outage. For example, if the RPO is one hour, the system must be recovered to a state no more than one hour before the failure occurred.

3. **Priority of Virtual Machines**: Assigning priorities to virtual machines (VMs) helps determine the order in which they are recovered after a disaster. Critical systems or applications essential for business operations are assigned high priority, ensuring they are restored first. Less critical systems may have lower priority, allowing them to be recovered after the high-priority systems are up and running.

Implementing an effective disaster recovery strategy involves a balance between RTO, RPO, and priority assignments to ensure that essential services are restored swiftly with minimal data loss, aligning with the organization's business continuity goals.

Priority of Virtual Machines: Identify the criticality of each virtual machine. High-priority VMs are essential for immediate business operations, so they should be restored first in case of a disaster. Lower priority VMs can be recovered in subsequent stages.

** Set Up Regular Backups:**

- **IBM Cloud Virtual Servers Backup:** Utilize IBM Cloud services to set up regular automated backups for your virtual machines. IBM Cloud provides various backup solutions, ensuring your data is securely stored and can be restored when needed.

- **Backup Tools or Scripts:** If your disaster recovery plan involves on-premises virtual machines, choose reliable backup tools compatible with your environment. Ensure these tools create regular backups and store them in a secure off-site location. Alternatively, develop backup scripts if you require custom solutions tailored to your specific needs.

Implementing a combination of IBM Cloud Virtual Servers backup services and on-premises backup tools/scripts will enhance your disaster recovery preparedness, meeting the defined RTO, RPO, and virtual machine priority requirements. Regularly test your backup and recovery processes to validate their effectiveness and make necessary adjustments based on the test outcomes.