## Define the disaster recovery strategy, including RTO, RPO, and priority of virtual machines.

## Set up regular backups of the on-premises virtual machine using backup tools or scripts.

**TEAMMEMBER:**

**Nepoliean.G**

**DEFNITION:**

**Building** a disaster recovery plan using IBM Cloud Virtual Serversinvolvesseveral key steps, including defining your disaster recovery strategy, determining Recovery Time Objective (RTO) and Recovery Point Objective (RPO), and setting up regular backups of on-premises virtual machines. Below, I'll outline the steps you can take to begin buildingyourdisasterrecovery plan.

**1.Define Disaster Recovery Strategy:**

* **Identify Critical Systems:**
* Determine which on-premises virtual machines are critical for your business operations. Not all systems may need the same level of recovery priority.
* **Select IBM Cloud Virtual Servers:**
* Choose the IBM Cloud Virtual Servers as the infrastructure for your disaster recovery solution. Ensure that it provides the necessary resources and scalability to meet your recovery needs

.

* **Geographical Redundancy:**
* Set up virtual servers in geographically redundant IBM Cloud data centers to ensure high availability. This redundancy helps to mitigate the risk of a single point of failure.
* **Failover Strategy:**
* Determine the failover strategy, including whether you want an active-passive or active-active setup. In active-passive, the standby environment only becomes active during a disaster, while in active-active, both environments are actively serving traffic.

**2. Define RTO and RPO:**

**Recovery Time Objective (RTO):**

**RTO** defines the maximum allowable downtime for a system. Determine how quickly you need to recover your systems after a disaster. For some systems, this could be minutes, while for others, it might be hours or days.

* **Recovery Point Objective (RPO):**
* RPO defines the maximum allowable data loss. It specifies how much data you are willing to lose during a recovery. For critical systems, you may need a near-zero RPO, while for less critical systems, you might tolerate some data loss.

**3. Prioritize Virtual Machines:**

* **Categorize Systems:**

Categorize your on-premises virtual machines into tiers based on their criticality. For example, Tier 1 systems might include mission-critical applications, while Tier 2 includes less critical systems.

* **Priority Levels:**
* Assign priority levels to each tier. This will determine the order in which you recover systems during a disaster. Critical systems with short RTO and RPO should have the highest priority.

**4. Set Up Regular Backups:**

* **Backup Tools or Scripts:**
* Choose and implement backup tools or scripts that are compatible with your on-premises virtual machines. IBM Cloud may have its backup solutions that can be integrated.
* **Backup Frequency:**
* Determine the frequency of backups based on your RPO. Critical systems might require real-time or near-real-time backups, while less critical systems may be backed up less frequently.
* **Offsite Backups:**
* Ensure that backups are stored offsite in a secure location, separate from the primary data center. This helps protect against disasters that might affect the primary location.

**5. Testing and Maintenance:**

* Regularly test your disaster recovery plan to ensure it works as expected. Test both the failover process and data recovery.
* Periodically review and update your disaster recovery plan to accommodate changes in your infrastructure and business requirements.

**6. Documentation:**

* Document the entire disaster recovery plan, including procedures, contact information, and key recovery steps. Ensure that all relevant team members have access to this documentation.

**7. \*\*Prioritize Virtual Machines:\*\***

* Identify the criticality of each virtual machine in your \*\*Test and Document:\*\*
* Test the backup and recovery processes to ensure they meet your RTO and RPO objectives.
* Document the entire disaster recovery plan, including backup schedules, procedures, and contact information.

**8. \*\*File Naming Convention:\*\***

* Follow the specified file naming convention (e.g., “CAD\_Phase3”) for your project documents.

**9. \*\*GitHub Submission:\*\***

* Upload your project file to your private GitHub account.
* Add the evaluators’ email IDs as collaborators on your GitHub repository to facilitate the evaluation process.

**10.\*\*Set Up Regular Backups:\*\***

* Environment. Prioritize them based on their importance to your business operations.
* Choose backup tools or scripts that are compatible with IBM Cloud Virtual Servers.
* Configure regular automated backups of your on-premises virtual machines. Ensure that the backups are consistent with your RPO
* Building a disaster recovery plan is a complex process that requires careful planning and continuous maintenance. It's essential to work closely with your IT team, consider the unique needs of your business, and stay up to date with best practices for disaster recovery in the cloud.

**\*\*\*\*\*\*\*\***

THANK**YOU🙏**