PHASE 3 DEVELOPMENT PART 1

DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

**Start building the disaster recovery plan using IBM Cloud Virtual Servers.**

* **Assessment and Risk Analysis:**

Begin by assessing your organization's specific needs and the potential risks and threats that could disrupt your operations. Consider factors such as natural disasters, hardware failures, cyberattacks, and data corruption.

* **Define Recovery Objectives:**

Determine the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for your applications and data. RTO represents how quickly you need to recover, while RPO defines how much data loss is acceptable.

* **Backup and Replication:**

IBM Cloud Virtual Servers offer various backup and replication options. Implement regular backups of your virtual server instances and data to ensure you have the necessary information for recovery. Explore options for real-time or near-real-time data replication.

* **Geographic Redundancy:**

Utilize IBM Cloud's multi-region capabilities to establish geographic redundancy. Spread your virtual servers across different data centers or regions to minimize the impact of a regional disaster.

* **Disaster Recovery Plan Documentation:**

Create a detailed document that outlines the entire disaster recovery plan. This should include contact information for team members, a step-by-step recovery process, and any critical configurations or scripts.

* **Failover and Failback Strategy:**

Determine how and when to fail over to your secondary virtual servers in the event of a disaster. Create a clear strategy for failing back to your primary environment once the issue is resolved.

* **Testing and Validation:**

Regularly test your disaster recovery plan to ensure it works as expected. Simulate different disaster scenarios to verify that your recovery procedures are effective and efficient.

* **Monitoring and Alerting:**

Implement robust monitoring tools that can detect issues in real-time. Set up alerts that notify your team when predefined thresholds are breached.

* **Response Team and Communication:**

Assemble a disaster recovery response team and establish clear communication channels. Define the roles and responsibilities of team members during a disaster.

* **Security and Compliance:**

Ensure that your disaster recovery plan complies with relevant security and regulatory requirements. Protect sensitive data during the recovery process.

* **Regular Updates and Maintenance:**

Continuously update and maintain your disaster recovery plan. As your infrastructure and applications evolve, your plan should adapt accordingly.

* **Training and Awareness:**

Train your team members in the execution of the disaster recovery plan. Ensure that all stakeholders are aware of their roles and responsibilities.

* **Documentation and Reporting:**

Keep thorough records of all recovery activities and create post-disaster reports to analyze the effectiveness of your plan and make necessary improvements.

* **Cloud Resource Allocation:**

Be prepared to allocate additional cloud resources in case of a disaster to handle increased workloads and traffic.

* **Vendor Support and Resources:**

Take advantage of IBM Cloud's support resources and services to assist in disaster recovery planning and execution.

* **Legal and Insurance Considerations:**

Consult with legal and insurance experts to ensure you have the appropriate coverage and legal safeguards in place.

**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.**

**1. Define RTO and RPO:**

* **Recovery Time Objective (RTO):**

This is the maximum allowable downtime for your virtual machines. It defines the time within which your systems must be restored after a disaster. For example, if your RTO is 4 hours, you aim to have your virtual machines operational within that time frame.

* **Recovery Point Objective (RPO):**

RPO represents the acceptable data loss in case of a disaster. It determines how frequently backups are taken. For instance, if your RPO is 1 hour, you can afford to lose no more than one hour's worth of data.

**2. Prioritize Virtual Machines:**

* Identify which virtual machines are critical to your business operations. These are typically the ones that host core applications, databases, and services. Assign priority levels to them (e.g., High, Medium, Low) based on their criticality.
* Prioritize based on business needs and the impact on revenue, customer service, and compliance. High-priority VMs should have shorter RTOs and lower RPOs.

**3. Backup Strategy for On-Premises Virtual Machines:**

* Choose backup tools or scripts that are suitable for your on-premises virtual machines. Popular options include Veeam, Acronis, and various built-in tools provided by virtualization platforms like VMware or Hyper-V.
* Configure and schedule regular backups for your virtual machines. Ensure that backups capture both the VM image and associated data.
* Consider implementing incremental or differential backups to reduce the backup window and storage requirements.

**4. Backup Frequency:**

* The backup frequency should align with your RPO. For example, if your RPO is 4 hours, you might set up backups every hour. Adjust this frequency for different priority levels. High-priority VMs may require more frequent backups.

**5. Backup Retention:**

* Define how long backups will be retained. Ensure that you have backups covering a reasonable historical timeframe, considering compliance requirements and the potential for discovering issues days or weeks after they occur.

**6. Backup Testing:**

* Regularly test your backups to ensure they are valid and can be used for recovery. This should be part of your disaster recovery plan.

**7. Secure Off-Site Storage:**

* Store backups in an off-site location, such as a secondary data center or a cloud storage solution. This provides redundancy and resilience in case of on-premises disasters.

**8. Automate Backup and Recovery:**

* Automate backup processes and ensure that the recovery process can be initiated quickly when needed. Automate testing procedures as well.

**9. Disaster Recovery Documentation:**

* Document your disaster recovery strategy, including RTO, RPO, and VM priorities. Make this documentation accessible to the disaster recovery team.

**10. Regular Review and Updates:**

* Regularly review and update your disaster recovery strategy to reflect changes in your infrastructure, applications, and business priorities.