Title: Disaster Recovery With IBM Cloud Virtual Server

PHASE – 3

DEVELOPMENT PART -1

A Disaster Recovery Plan (DRP) is a documented strategy outlining the procedures an organization follows to recover and protect its IT infrastructure in the event of a disaster. This plan is essential for minimizing downtime, data loss, and financial impact during unforeseen events.

Disaster Recovery Strategy:

1. RTO (Recovery Time Objective):

Define the acceptable downtime for the services. For example, if RTO is set to 4 hours, it means that services should be restored within 4 hours after a disaster occurs.

2. RPO (Recovery Point Objective):

Determine the maximum amount of data loss that is acceptable. For instance, if RPO is set to 1 hour, it means that no more than 1 hour's worth of data can be lost in the event of a disaster.

3. Priority of Virtual Machines:

Categorize virtual machines based on their criticality to business operations. For example:

Priority 1 (High): These are mission-critical systems with little tolerance for downtime.

Priority 2 (Medium): These are important systems but can tolerate a bit of downtime.

Priority 3 (Low): These systems are less critical and can handle extended downtime.

RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are critical parameters in any disaster recovery strategy. They define the acceptable levels of downtime and data loss in the event of a disaster, helping organizations prioritize their recovery efforts.

Recovery Time Objective (RTO):

RTO refers to the maximum amount of time that a system or service can be down before it starts causing significant harm to the business. It represents the acceptable downtime for a service or application.

Example: If a business has an RTO of 4 hours, it means that in the event of a disaster, the affected service or application must be restored and operational within 4 hours.

Factors influencing RTO:

- Criticality of the system or service.
- Complexity of recovery processes.
- Availability of resources and technology.
- Business impact of prolonged downtime.

Recovery Point Objective (RPO):

RPO is the maximum tolerable amount of data loss measured in time. It signifies the point in time to which data must be recovered after a disaster. It essentially defines how much data the organization can afford to lose.

Example: If an organization has an RPO of 1 hour, it means that in case of a disaster, they can't afford to lose more than 1 hour's worth of data.

Factors influencing RPO:

- Frequency of data backups or snapshots.
- Rate of data change within applications.
- Importance of real-time data updates.
- Relationship between RTO and RPO:

Alignment: RTO and RPO should be closely aligned. In many cases, RPO will influence the RTO. If a very low RPO is required (meaning minimal data loss is acceptable), it may dictate a shorter RTO because more frequent backups or replication will be necessary.

Balancing Act: Achieving a very low RTO and RPO can be costly. There's a trade-off between the cost of implementing high-availability solutions and the potential loss incurred from extended downtime or data loss.

Application Dependency: Different applications may have different RTO and RPO requirements. Mission-critical applications may require near-zero RTO and very low RPO, while less critical services may have more relaxed objectives.

Technology and Infrastructure: The choice of technology and infrastructure (like cloud services, backup solutions, etc.) greatly influences the ability to meet RTO and RPO targets.

Testing and Validation: Regular testing and validation are essential to ensure that the set RTO and RPO objectives can be met in practice.

Setting Up Regular Backups:

IBM Cloud Backup Service:

Utilize IBM Cloud's native backup service to automate backups of virtual machines. This service provides options for scheduling, retention policies, and easy recovery.

Custom Scripts for On-Premises Backups:

Develop custom scripts to perform regular backups of on-premises virtual machines. These scripts can leverage tools like Veeam, Acronis, or native OS backup utilities.

Backup Frequency:

Define the frequency of backups based on the RPO. For example, if RPO is 1 hour, backups should be taken at least every hour.

Retention Policies:

Determine how long backups will be retained. This should align with compliance requirements and business needs. For example, keep daily backups for 7 days, weekly backups for 4 weeks, and monthly backups for 6 months.

Offsite Storage:

Ensure that backups are stored in an offsite location, either in a different physical location or in a cloud storage solution. This safeguards against disasters that might affect the primary site.

Regular Testing and Validation:

Periodically perform recovery tests to ensure that backups can be successfully restored. This helps identify and address any issues in the backup process.

Additional Considerations:

Failover and Failback Procedures:

Develop detailed procedures for failing over services to the IBM Cloud Virtual Servers in the event of a disaster. Also, outline steps for failing back to on-premises infrastructure once the disaster is resolved.

Monitoring and Alerting:

Implement robust monitoring solutions to keep track of the health and availability of both on-premises and cloud-based resources. Set up alerts for any anomalies or outages.

Documentation and Communication:

Document the entire disaster recovery plan, including procedures, contacts, and configurations. Ensure that all stakeholders are aware of the plan and their roles in the event of a disaster.

Compliance and Regulatory Considerations:

Ensure that the disaster recovery plan aligns with any industry-specific compliance requirements (e.g., HIPAA, GDPR) that may apply to your organization.

By following these steps, we'll establish a robust disaster recovery plan using IBM Cloud Virtual Servers, ensuring the resilience of your critical services in the face of unforeseen events.