DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

presented by :Ishwarya.K

Project Scope and Objectives:

Clearly define the scope of the project.

Outline specific objectives, such as creating a disaster recovery plan, setting up backup strategies, and ensuring minimal downtime.

Stakeholder Identification

Identify all stakeholders involved, including IT teams, management, and any external partners or vendors.

Resource Allocation: Determine the resources needed for the project, including personnel, budget, and technology.

Timeline and Milestones:

Create a project timeline with key milestones, ensuring realistic deadlines for each phase.

Project Team Formation:

Assemble a project team with the necessary skills and expertise in disaster recovery planning and IBM Cloud Virtual Servers.

Research and Planning:

Conduct thorough research on disaster recovery best practices, IBM Cloud Virtual Servers capabilities, and any specific requirements for your environment.

Disaster Recovery Strategy:

Define the overall disaster recovery strategy, including backup frequency, replication methods, and failover procedures.

Backup and Replication Configuration:

Implement backup strategies and configure replication mechanisms according to the defined strategy

Testing Procedures:

Develop test scenarios and procedures to validate the effectiveness of the disaster recovery plan.

Documentation:

Create comprehensive documentation for all aspects of the project, including configurations, procedures, and recovery plans.

Training and Awareness:

Provide training to relevant stakeholders on executing the disaster recovery plan.

Testing and Validation:

Conduct thorough testing of the disaster recovery plan using simulated disaster scenarios.

Monitoring and Maintenance:

- Set up monitoring tools and establish regular maintenance procedures for ongoing health and performance checks.

Communication Plan:

- Establish a protocol for notifying stakeholders in the event of a disaster and provide regular updates on the project's progress.

Review and Approval:

- Seek feedback from stakeholders and make any necessary adjustments based on their input.

Final Testing and Deployment:

- Conduct a final round of testing to ensure all components of the disaster recovery plan are functioning as expected.

Go-Live and Implementation:

- Deploy the disaster recovery plan into production, and monitor its performance in real-world scenarios.

Post-Implementation Review:

- Evaluate the project's success, identify lessons learned, and document any improvements for future reference.

Disaster Recovery Strategy:

Define Objectives:

Gather input from stakeholders to determine the specific objectives of your disaster recovery plan. This could include goals like minimizing downtime, preserving critical data, etc.

Set RTO and RPO:

Determine the acceptable Recovery Time Objective (RTO), which specifies how quickly systems need to be restored, and the Recovery Point Objective (RPO), indicating how much data loss is acceptable.

Document Strategy:

-Clearly document the disaster recovery strategy, including objectives, RTO, and RPO. Ensure all stakeholders understand and approve of the strategy.

Backup Configuration:

Select Backup Tools:

Choose appropriate backup tools and technologies compatible with your on-premises virtual machine environment. This could involve using built-in backup features or third-party solutions.

Define Backup Schedule:

Establish a regular backup schedule that captures critical data and configurations. Consider factors like frequency, time of day, and retention policies.

Test Backups:

- Regularly test backups to ensure they are successful and can be restored effectively.

Replication Setup:

Select Replication Mechanism:

Choose the appropriate replication method (e.g., synchronous, asynchronous) based on your RPO and RTO requirements.

Configure Replication:

Set up replication from your on-premises virtual machine to IBM Cloud Virtual Servers. Ensure data consistency and synchronization.

Monitor Replication Status:

Implement monitoring tools to track the status of replication processes and detect any issues promptly.

Recovery Testing:

Plan Test Scenarios:

Develop a range of disaster scenarios (e.g., hardware failure, data corruption) to validate the recovery process.

Conduct Recovery Tests:

Execute the planned scenarios and assess how well the recovery process works. Document any issues encountered and make necessary adjustments.

Iterate and Improve:

Based on test results, refine the disaster recovery plan and conduct additional tests as needed.

Business Continuity:

Alignment with Business Goals:

Ensure that the disaster recovery plan aligns with the broader business continuity strategy and supports the organization's overall goals and objectives.

Stakeholder Communication:

Communicate the importance of business continuity and disaster recovery to all relevant stakeholders. Obtain buy-in and support from management.

Integration with IT Governance:

Ensure that the disaster recovery plan complies with any relevant industry standards or regulatory requirements.

THANK YOU