Cloud Application Development

Phase -3 : Submission Document

IBM: CAD101

Project 8:

Disaster Recovery with IBM Cloud Virtual Servers

Problem Statement:

Safeguard business operations with IBM Cloud Virtual Servers. Create a disaster recovery plan for an on-premises virtual machine, ensuring continuity in unforeseen events. Test and validate the recovery process to guarantee minimal downtime. Become the guardian of business continuity, securing the future of your organization

Phase3:

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

SOLUTION:

Step 1:

Define Disaster Recovery Strategy

1.1 Disaster Recovery Objectives:

RTO (Recovery Time Objective):

The RTO is the maximum acceptable downtime for your critical services or applications. It indicates how quickly you need to recover after a disaster.

RPO (Recovery Point Objective):

The RPO is the maximum acceptable amount of data loss measured in time. It defines the point in time to which you can recover your data.

1.2 Virtual Machines Classification:

Priority Levels:

Critical: These are the most essential VMs for your business operations. They should have the shortest RTO and RPO.

High: Important VMs that are necessary for continued operations, but not as critical as the critical category.

Medium: VMs that are important but can wait a bit longer for recovery.

Low: Less critical VMs, which can be recovered later if necessary.

Step 2: IBM Cloud Resources Setup

2.1 Establish IBM Cloud Account:

Ensure you have a valid IBM Cloud account with access to the Virtual Servers and other relevant services.

2.2 Virtual Server Deployment:

Deploy the necessary Virtual Servers in different availability zones or regions. This ensures redundancy and minimizes the risk of a single point of failure.

2.3 Networking Setup:

Configure Virtual LANs (VLANs) and subnets to ensure proper communication between the servers. Set up load balancers for critical applications for high availability.

2.4 Data Backup and Replication:

Implement regular backups and use IBM Cloud Object Storage or other services for data replication. This will help in achieving the defined RPO.

Step 3: Disaster Recovery Plan Documentation

3.1 Detailed Procedures:

Document step-by-step procedures for the following scenarios:

Initial Setup

Routine Backups

Recovery Process

Failover Process

Failback Process

3.2 Contact Information:

Include contact details of key personnel responsible for executing the disaster recovery plan.

3.3 Escalation Plan:

Define the chain of command and escalation procedures in case the primary contacts are unavailable.

Step 4: Testing and Maintenance

4.1 Regular Testing:

Perform scheduled disaster recovery drills to ensure the plan works as expected. This helps in identifying any gaps or weaknesses.

4.2 Updates and Maintenance:

Regularly review and update the disaster recovery plan to account for changes in infrastructure, applications, or business processes.

Step 5: Monitoring and Alerts

5.1 Monitoring Tools:

Utilize IBM Cloud monitoring tools to keep an eye on the health and performance of your Virtual Servers.

5.2 Alerting System:

Set up alerts for critical events like server failures, high resource usage, or network issues.

Step 6: Employee Training and Awareness

Ensure that all relevant staff members are aware of the disaster recovery plan and their roles in executing it.

Step 7: Compliance and Regulations

Ensure that your disaster recovery plan complies with any industry-specific regulations or requirements.

Remember, this is a high-level overview. You'll need to delve deeper into the specific configurations, tools, and procedures based on your exact requirements and the capabilities of IBM Cloud Virtual Servers.

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

Step 1: Select Backup Tools or Scripts

1.1 Choose Backup Software:

Select a backup software or solution that supports on-premises virtual machines. Popular options include Veeam, Commvault, Acronis, and Windows Server Backup.

1.2 Consider Backup Scripts:

If you prefer a more customized approach, you can write backup scripts using tools like PowerShell (for Windows) or shell scripts (for Linux).

Step 2: Identify Data to Back Up

2.1 Critical Data:

Identify the files, folders, databases, and system configurations that need to be backed up. Focus on critical data for your business operations.

2.2 Application-Specific Considerations:

For applications running on your virtual machines, ensure you understand any special considerations for backup and recovery.

Step 3: Determine Backup Schedule

3.1 Frequency:

Decide how often you want to perform backups. This could range from daily to weekly, depending on your business requirements.

3.2 Full vs. Incremental Backups:

Choose between full backups (copies all selected data) and incremental backups (copies only the data that has changed since the last backup).

Step 4: Set Up Backup Storage

4.1 Storage Location:

Determine where you'll store your backups. This could be an external hard drive, a network-attached storage (NAS) device, a dedicated backup server, or a cloud storage service.

4.2 Ensure Adequate Storage Capacity:

Make sure you have enough storage space to accommodate your backups, especially considering retention policies.

Step 5: Configure Backup Software or Scripts

5.1 Install and Configure Backup Software:

If using backup software, follow the vendor's instructions to install and configure it. Set up backup schedules, retention policies, and storage locations.

5.2 Write Backup Scripts (if applicable):

If using scripts, write scripts to automate the backup process. Ensure they are set up to run at the specified intervals.

Step 6: Test Backups

6.1 Perform Test Restorations:

Regularly test your backups by performing test restorations. This ensures that your backup process is working correctly and that you can recover data when needed.

Step 7: Monitor and Maintain Backups

7.1 Monitoring:

Keep an eye on backup logs and alerts to ensure backups are running as scheduled and there are no errors.

7.2 Periodic Reviews:

Regularly review your backup strategy to ensure it meets your evolving business needs. Make adjustments as necessary.

Step 8: Document the Backup Process

8.1 Document Procedures:

Create detailed documentation of the backup process, including steps for backup initiation, restoration, and any troubleshooting procedures.

8.2 Contact Information:

Include contact details for key personnel responsible for managing backups.

Remember, it's crucial to regularly validate your backups to ensure they're reliable in the event of a disaster or data loss scenario. Additionally, consider encryption and off-site storage options for added security and redundancy.