Disaster Recovery with IBM Cloud Virtual Servers
Phase 3

Abstract :

A 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.

IBM Cloud Virtual Servers :

IBM Cloud Virtual Servers, previously known as IBM SoftLayer, is an Infrastructure as a Service (IaaS) offering by IBM Cloud. It provides on-demand, scalable virtual servers that allow businesses and developers to run and manage their applications and workloads in the cloud.

1.Virtualization Technology : IBM Cloud Virtual Servers are built on virtualization technology, allowing users to create and manage virtual machines (VMs) with various operating systems, such as Linux and Windows.

2. Storage Options : IBM Cloud provides a variety of storage options, including local and network-attached storage (NAS). You can choose the storage type that best fits your performance and capacity requirements.

How to use disaster recovery plan :

Using a disaster recovery plan (DRP) for IBM Cloud Virtual Servers involves a series of steps and actions to ensure the availability, continuity, and recovery of your virtual server-based applications and data in the event of a disaster or system failure. Here's how to use a disaster recovery plan in the context of IBM Cloud Virtual servers .

1. Preparation and Documentation: Before a disaster occurs, ensure that your DRP is well-documented and readily accessible. Your team should be trained on its contents and procedures.

2.Identification of Disaster: Promptly identify the disaster or failure, whether it's a data center issue, server failure, or another critical incident that impacts your IBM Cloud Virtual Servers.

3.Data Restoration: Restore data from the latest backup or snapshot, ensuring that it aligns with your defined Recovery Point Objective (RPO).

4.Server Failover: Activate secondary or backup virtual servers as per the failover strategy. Ensure that the Recovery Time Objective (RTO) is met and applications are back online.

Disaster Recovery Strategy :

A disaster recovery strategy is a comprehensive plan that outlines how an organization will respond to and recover from a significant disruptive event, such as a natural disaster, system failure, or cyberattack. Central to this strategy are three critical elements : Recovery Time Objective (RTO), Recovery Point Objective (RPO), and the priority of virtual machines.

Recovery Time Objective (RTO):

RTO is a defined time frame within which an organization aims to recover its systems and applications following a disaster or disruption. It represents the maximum tolerable downtime for specific applications or systems. The RTO is a critical metric that influences how quickly recovery actions need to be executed.

For example : an organization might set an RTO of 4 hours for a critical e-commerce application. This means that, in the event of a disaster, the organization must have the application fully operational within 4 hours to minimize business disruption.

Recovery Point Objective (RPO):

RPO is the maximum allowable data loss in the event of a disaster or system failure. It defines the point in time to which data must be restored to ensure business continuity. RPO is closely tied to data replication and backup strategies.

Consider an organization with an RPO of 1 hour for a customer database. This means that, in the event of a disaster, the organization can afford to lose no more than 1 hour of data.

Data backups and replication mechanisms must ensure that data is protected up to that point.

Priority of Virtual Machines:

Virtual machines are often prioritized based on their criticality to business operations. Prioritization helps ensure that resources and efforts are focused on the most essential systems and applications during recovery efforts.

For example, a business might categorize its virtual machines into three priority levels:

High Priority: These virtual machines host mission-critical applications or services. They have the shortest RTO, typically near real-time, and a very low RPO.

Medium Priority: These VMs support important but non-mission-critical functions. They have a moderate RTO and a somewhat higher RPO.

Low Priority: These VMs are for non-essential or non-time-sensitive tasks. They have a longer RTO and a more flexible RPO.

Regular backups of the on-premises virtual machine using backup tools (or) scripts :

1. **Select Backup Tools or Scripts:** Choose backup software or scripts that are compatible with your virtualization platform and meet your backup needs. Popular tools include

Veeam, Backup Exec, and Acronis. If you prefer scripts, consider using PowerShell or other scripting languages.

2. Install and Configure Backup Software : Install the chosen backup software on a dedicated backup server or a separate virtual machine within your on-premises environment. Configure the software according to your needs and the software's documentation.

3. Define Backup Policies: Create backup policies that specify when and how often backups should occur. You can set daily, weekly, or monthly backup schedules, depending on your requirements.

4. Identify Backup Targets: Determine where you want to store your backups. Options include local storage, network-attached storage (NAS), and off-site or cloud storage for disaster recovery.

5. Configure Backup Sources: Identify the virtual machines you want to back up. Set up the backup software or scripts to recognize these VMs as backup sources.

6. Set Retention Policies: Define how long you want to retain backup data. Set retention policies to ensure that you keep backups for an appropriate duration. Typically, you'll have daily, weekly, and monthly retention policies.

7. Test Backup and Restore Procedures: Regularly test backup and restore procedures to ensure that you can recover

virtual machines and data when needed. Verify that your backups are valid and usable.

8. Monitor Backup Status: Implement monitoring and alerting for backup jobs. Configure notifications to alert you when backups fail or encounter issues.

9. Automate Backup Execution: Automate the backup process to run at specified times without manual intervention. Backup software often provides scheduling and automation features.

10. Implement Incremental Backups: Use incremental or differential backup strategies to reduce storage requirements and speed up backup times. These methods back up only the changed data since the last backup.

11. Secure Backup Data: Ensure that backup data is stored securely. Encrypt backup files to protect sensitive information and consider off-site storage or cloud-based backups for added security.

12. Regularly Update and Test Backup Software: Keep your backup software up to date with the latest patches and updates. Regularly test the performance and reliability of your backups.

13. Document Backup Procedures: Document the backup and restore procedures, including step-by-step instructions.

This documentation is vital for staff continuity and disaster recovery.

14. **Implement Off-Site Backups**: As part of your disaster recovery strategy, consider replicating backups to an off-site location or using cloud-based backups. This provides additional protection in case of on-premises disasters.

15. **Review and Revise**: Periodically review your backup strategy to ensure it aligns with your changing needs and the evolving technology landscape.

Script of IBM Cloud Server :

If you want to perform regular backups of virtual machines hosted on IBM Cloud Virtual Servers, you can use a combination of IBM Cloud features and tools.

```
 # Log in to IBM Cloud (if not already logged in)
ibmcloud login


# Target the specific resource group and region where your virtual server is located
ibmcloud target -g <resource_group> -r <region>


# Create a snapshot of a virtual server instance
```

```
ibmcloud is snapshot-create <virtual_server_instance_id>
--name <snapshot_name>
```

Below is a general approach to performing backups using IBM Cloud Virtual Servers:

1. IBM Cloud Virtual Servers Snapshots
2. Create a Snapshot
3. Backup Scheduling
4. Retention Policies
5. Automation and Scripts

EXAMPLE SCRIPT :

A simple script to perform regular backups of a virtual machine using PowerShell on a Windows environment. This script demonstrates how you can create a backup of a virtual machine and save it to a specified location.

```
# Define variables

$VMName = "YourVirtualMachineName"

$BackupLocation = "C:\Backups"

$BackupFileName = "$VMName-Backup-$(Get-Date -
Format 'yyyyMMdd-HHmmss').vhdx"
```

```
# Create a checkpoint (snapshot) of the virtual machine
Checkpoint-VM -Name $VMName -SnapshotName "Backup"

# Export the virtual machine checkpoint to a backup file
Export-VMSnapshot -Name $VMName -SnapshotName "Backup" -Path $BackupLocation -Name $BackupFileName

# Remove the checkpoint (optional, if you don't want to keep the snapshot)
Remove-VMSnapshot -Name $VMName -SnapshotName "Backup"

# Clean up old backups (optional, if needed)
# For example, you can keep a certain number of backups and delete older ones

# List backup files
$BackupFiles = Get-ChildItem -Path $BackupLocation

# Sort the backup files by creation time
$BackupFiles | Sort-Object CreationTime -Descending
```

```
# Keep a specified number of backups (e.g., keep the latest 5 backups)
$BackupsToKeep = 5

if ($BackupFiles.Count -gt $BackupsToKeep) {
    $BackupsToDelete = $BackupFiles | Select-Object -Skip $BackupsToKeep
    $BackupsToDelete | ForEach-Object {
        Remove-Item $_.FullName
    }
}

# Output status or send notifications (optional)
Write-Host "Backup of $VMName completed and stored in $BackupLocation"
# You can also add email notifications, logging, or other actions here
```