Phase 3: Development part 1

Define the disaster recovery strategy, including RTO, RPO, and priority of virtual machines.

- disaster recovery (DR) strategy is a comprehensive plan that outlines the steps an organization will take to recover its IT infrastructure and operations in the event of a disaster. The goal of a DR strategy is to minimize downtime and data loss, and to ensure that the organization can resume normal operations as quickly as possible.
- Key elements of a disaster recovery strategy
- A disaster recovery strategy should include the following key elements:

Recovery Time Objective (RTO):

- The RTO is the maximum amount of time that an organization can tolerate its IT systems being down before it starts to suffer significant financial or operational losses.
- Recovery Point Objective (RPO): The RPO is the maximum amount of data that an organization can afford to lose in a disaster.
- Priority of virtual machines: The priority of virtual machines (VMs) is a ranking of the importance of each VM to the organization's operations. VMs that are critical to business operations should be given a higher priority than VMs that are less critical.

Developing a disaster recovery strategy

The following steps can be used to develop a disaster recovery strategy:

Identify critical IT systems and applications:

- The first step is to identify the IT systems and applications that are critical to the organization's operations. These systems should be given the highest priority in the DR plan.

Determine RTO and RPO:

- The next step is to determine the RTO and RPO for each critical system. The RTO and RPO should be based on the organization's tolerance for downtime and data loss.
- Select a DR solution: There are a number of different DR solutions available, including replication, backup and restore, and cloud-based DR. The organization should select the solution that best meets its needs and budget.

Test the DR plan:

- The DR plan should be tested regularly to ensure that it is effective. Testing should include both simulated disasters and actual failovers.

Prioritizing virtual machines

The priority of VMs should be based on the following factors:

- Criticality of the VM to business operations: VMs that are critical to business operations should be given a higher priority than VMs that are less critical.
- Availability of other resources: If there are other resources available to perform the same function as a VM, then that VM can be given a lower priority.

<u>Cost of downtime:</u> The cost of downtime for a VM should also be considered when prioritizing VMs. VMs that have a high cost of downtime should be given a higher priority.

Example of a disaster recovery strategy:

- An example of a disaster recovery strategy for a company that runs an e-commerce website might be as follows:

1. RTO: 4 hours
2. RPO: 1 hour

<u>Priority of virtual machines:</u>

1. Web server VM
2. Database server VM
3. Application server VM

- This DR strategy would ensure that the company's e-commerce website is back up and running within 4 hours of a disaster, and that no more than 1 hour of data is lost. The web server VM is given the highest priority because it is the most critical to the company's operations. The database server VM is given the second highest priority because it stores the company's data. The application server VM is given the lowest priority because it can be replaced by another VM if necessary.
- Now, to set up regular backups for on-premises virtual machines, you can use backup tools or scripts.
- Here's a high-level overview of how to set up backups using a script:

```
#!/bin/bash

# Set variables for your environment

Vm_name=”YourVMName”

Backup_location=”/path/to/backup/location”

Current_date=$(date +”%Y%m%d%H%M%S”)

# Create a snapshot of the virtual machine

Az vm stop –resource-group YourResourceGroup –name $vm_name

Az vm snapshot –resource-group YourResourceGroup –name $vm_name –snapshot-name
“${vm_name}_$current_date”

# Copy the snapshot to the backup location

Az storage blob copy start-batch –destination-container $backup_location –destination-path
“${vm_name}_$current_date.vhd” –destination-blob “${vm_name}_$current_date.vhd” –source-
```

```
container vhds –source-blob “${vm_name}_$current_date.vhd” –source-uri $(az snapshot show –
name “${vm_name}_$current_date” –resource-group YourResourceGroup –query [uri] –output tsv)


# Delete older snapshots to manage storage costs

# Optionally, you can retain a certain number of snapshots


# Restart the virtual machine

Az vm start –resource-group YourResourceGroup –name $vm_name
```

Conclusion:

- A disaster recovery strategy is an essential part of any organization’s IT plan. By developing and testing a DR strategy, organizations can minimize downtime and data loss in the event of a disaster.

Here are some of the key components of a disaster recovery strategy:

- Risk assessment: Identify and assess the potential risks to the organization’s IT infrastructure and operations.
- Business impact analysis: Determine the impact of a disaster on the organization’s business operations.

Disaster recovery plan:

- Develop a detailed plan for restoring IT systems and applications in the event of a disaster.

Testing and validation:

- Regularly test and validate the disaster recovery plan to ensure that it is effective.

Training: Train employees on their roles and responsibilities in the event of a disaster.

Communication:

- Establish a communication plan for keeping employees, customers, and other stakeholders informed in the event of a disaster.
- By implementing a comprehensive disaster recovery strategy, organizations can minimize the impact of a disaster and ensure that they can resume normal operations as quickly as possible.

Choose a DR solution:

- Select a DR solution that meets the organization’s RTO and RPO requirements.

Test and refine the DR plan:

- Regularly test the DR plan to ensure that it is effective and up-to-date.

Prioritizing virtual machines:

- Tier 1 VMs: These are the most critical VMs and should be recovered first. They support essential business functions and have a low tolerance for downtime.
- Tier 2 VMs: These VMs are important but not as critical as Tier 1 VMs. They can tolerate some downtime but should be recovered as soon as possible.
- Tier 3 VMs: These VMs are the least critical and can tolerate longer downtime. They can be recovered after Tier 1 and Tier 2 VMs have been restored.

Example of a disaster recovery strategy:

- An e-commerce company has an RTO of 4 hours and an RPO of 1 hour for its website. This means that the company must be able to restore its website within 4 hours of a disaster, and it can only afford to lose 1 hour of data. The company's DR plan prioritizes the recovery of its web servers, database servers, and application servers.
- By having a well-defined disaster recovery strategy, organizations can minimize the impact of disasters and ensure business continuity.

Setting Up Regular Backups:

- To ensure a robust disaster recovery strategy, regular backups are essential. You can use backup tools or scripts to automate this process. Here's an example using PowerShell for Hyper-V VMs on-premises:

```
# Define your backup location
$backupLocation = “D:\Backup”

# Get a list of VMs to backup
$vmList = Get-VM

# Loop through VMs and create backups
Foreach ($vm in $vmList) {
   $vmName = $vm.Name
   $backupFileName = “$backupLocation\$vmName-$(Get-Date -Format ‘yyyyMMdd-HHmmss’).vhdx”
   Backup-VM -Name $vmName -Path $backupFileName
}

# Set up a schedule (e.g., daily) to run this script using Task Scheduler
```

1. **Choose Backup Tools or Scripts:**

- Select backup tools or scripts compatible with your virtual machine environment.
- Consider features like incremental backups, compression, and encryption.

2. **Schedule Backup Frequency:**

- Determine backup frequency based on RPO requirements for each virtual machine tier.
- Schedule backups during off-peak hours to minimize performance impact.

3. **Automate Backup Processes:**

- Utilize automation tools or scripts to streamline backup tasks.
- Integrate backups with monitoring systems for proactive alerts and notifications.

4. **Verify Backup Integrity:**

- Regularly test backups to ensure data integrity and recoverability.
- Perform test restores to validate the restoration process and data consistency.

5. **Store Backups Securely:**

- Maintain multiple copies of backups in geographically separate locations.
- Implement secure storage practices to protect backups from unauthorized access.

6. **Document Backup Procedures:**

- Create comprehensive documentation outlining backup processes and schedules.
- Include instructions for restoring virtual machines from backups.
- Regularly review and update documentation as needed.