AGENDA

1. Introduction
2. Disaster recovery strategies
3. RTO
4. RPO
5. Backup tools and scripts for virtual machine
6. Building a disaster recovery plan
7. Conclusion

INTRODUCTION:

➢ A disaster recovery strategy is a plan to restore and resume critical business functions after a disruptive event, such as a natural disaster, cyberattack, or pandemic.

➢ It is a vital component of business resilience, which is the ability to adapt and recover from any challenge.

DISASTER STRATAGIES

The disaster strategy should include Risk assessment, Recovery objectives , Recovery strategies , Incident response, Business continuity , Lessons learned.

RTO

- ➤ RTO (the Recovery Time Objective), is a metric that defines the time to recover your IT infrastructure and services following a disaster to ensure business continuity.
- ➤ If during real-life disaster recovery, you go over the given time-frame, you should either reconsider the RTO calculations or update your disaster recovery plan and procedures
- ➤ To calculate RTO, consider these factors:
- ➤ The cost per hour of outage.
- ➤ The importance and priority of individual systems.
- ➤ Steps required to recover from a disaster (including individual components and processes)
- ➤ Available budget and resources.

RPO

➢ RPO, or Recovery Point Objective, is a measure of the maximum tolerable amount of data that the business can afford to lose during a disaster. It also helps you measure how long it can take between the last data backup and a disaster without seriously damaging your business. RPO is useful for determining how often to perform data backups.

➢ Here are the factors for determining your RPO:

➢ The maximum tolerable amount of data loss that your organization can sustain.

➢ The cost of lost data.

➢ Available budget and resources.

BACKUP TOOLS AND SCRIPTS OF VIRTUAL MACHINE

To set up regular backups of on-premises virtual machines, you can follow these steps:

1. Select Backup Tools or Scripts

2. Define Backup Policies

3. Backup Schedule

4. Offsite Storage

5. Test Backups

6. Monitoring and Alerts

7. Documentation

8. Regular Review

Powershell Script for Backing Up Virtual Machines:

Define variables

$VMName = "YourVirtualMachineName"

$BackupLocation = "C:\Backup" # Change this to your desired backup location

$BackupTime = Get-Date

$BackupTimeFormatted = Get-Date –Format "yyyyMMddHHmmss"

Create a backup folder for this backup

$BackupFolder = Join-Path –Path

$BackupLocation –ChildPath

"Backup_ $BackupTimeFormatted"New-Item –Path

$BackupFolder –ItemType Directory

Execute the backup command specific to your backup tool

Example for Veeam Backup & Replication

Replace with your backup tool's specific command or script

Start-VBRZip –Entity

$VMName –Folder $BackupFolder

Add error handling, notifications, and retention policy as needed

This script creates a new backup folder for each backup. Retention policies can be added to manage backups over time

Schedule this script to run regularly, e.g., using Task Scheduler in Windows.

1. **Customization:** Replace $VM Name with the name of your virtual machine. Modify $Backup Location to specify the desired backup destination. Replace the Start-VBRZip command with the appropriate backup command for your chosen backup tool.
2. **Automation and Scheduling:** Schedule this script to run at regular intervals using a tool like Task Scheduler on a Windows system. Ensure that the script runs with appropriate permissions to access the virtual machine and write backups to the specified location.
3. **Error Handling and Notifications:** Add error-handling logic to handle backup failures. Consider sending email notifications or logs to notify administrators of backup status.
4. **Retention Policy:** Implement a retention policy to manage the number and age of backup ps, ensuring that you keep backups within your desired RPO and RTO requirements

Conclusion

The advantages of disaster recovery in the cloud are more significant than the drawbacks. Using a cloud-based DR strategy, you can benefit from high scalability, automation, cost-effectiveness, flexibility, reliability, and the ability to deploy DR sites in different geographical regions while eliminating the dependency on physical hardware. To make it more effective, proper planning and testing are required to ensure that the solution fits organizational needs and requirements.

THANK YOU

DEPARTMENT OF CSE

ARUNAI
Engineering College
Tiruvannamalai, Tamil Nadu