

ARUNAI ENGINEERING COLLEGE

CODE :5104



Department Of Information Technology

Disaster Recovery With IBM Cloud Virtual Server



PRESENTED BY:R.Dhanalakshmi
GUIDED BY:K.Hari Priya

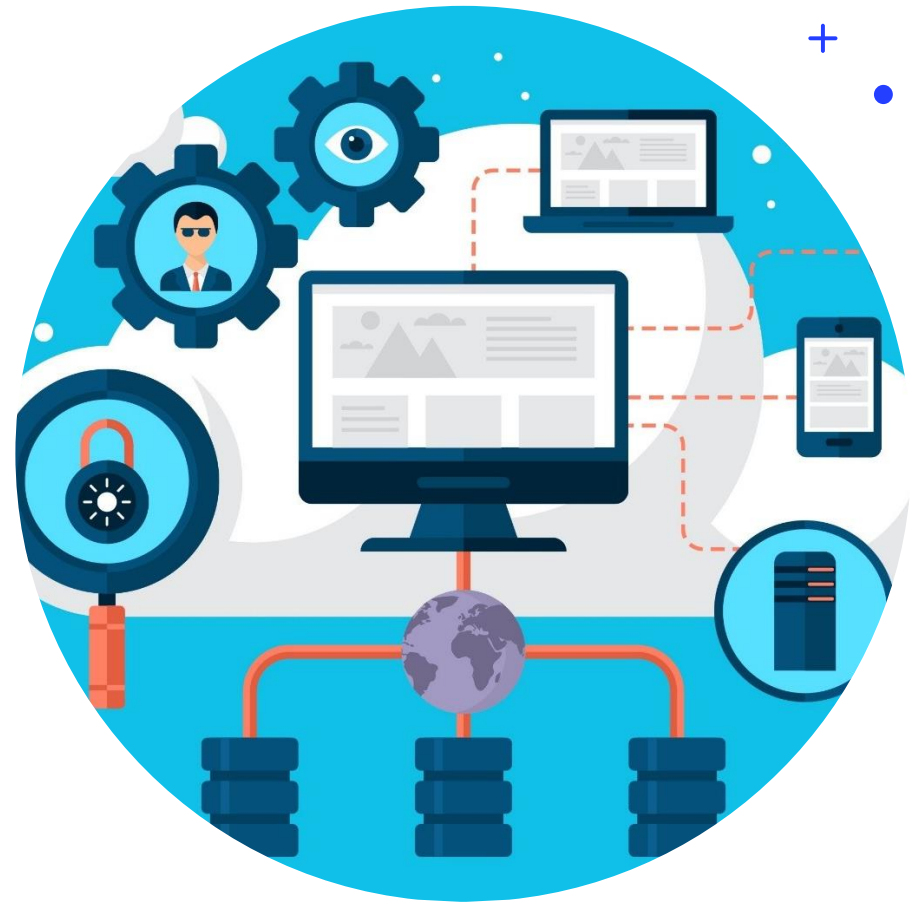


AGENDA

- Introduction
- Design thinking
- Project Objective
- Recovery Time Objective
- Source Code
- Output
- Recovery Point Objective
- Summary

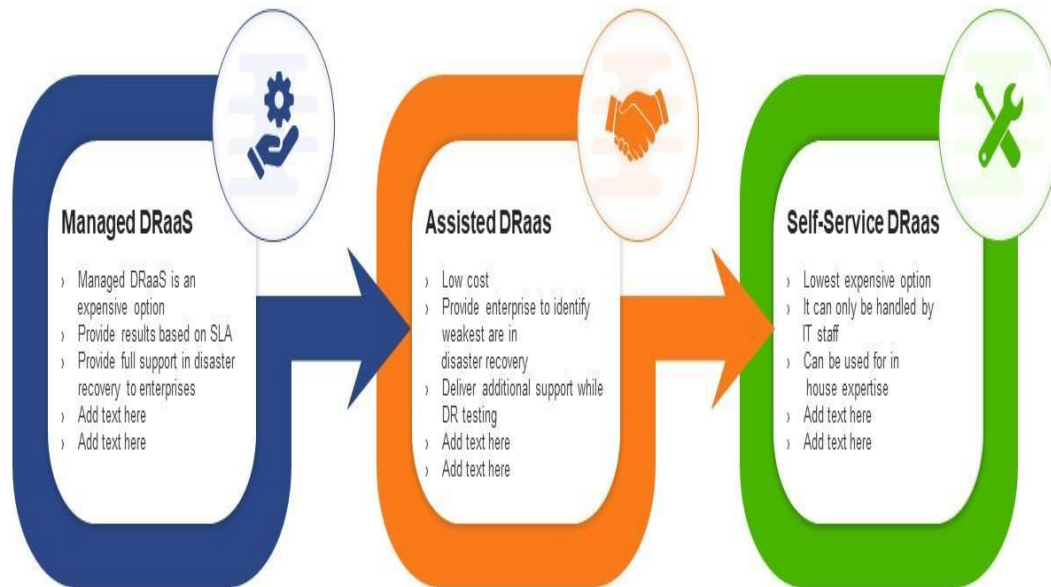
Introduction

Disaster recovery with IBM Cloud Virtual Servers involves planning and implementing strategies to ensure the availability and resilience of your virtual server instances in the event of unexpected disruptions or disasters. IBM Cloud offers a range of services and features that can help you establish a robust disaster recovery plan for your virtual servers.



Cloud Disaster Recovery Options for Enterprise Data Protection

The following slide illustrates the cloud disaster recovery options which include managed DRaaS, Assisted DRaaS and self-service DRaaS.



This slide is 100% editable. Adapt it to your needs and capture your audience's attention.



Design Thinking

Empathize: Understand the needs and challenges of IBM's cloud clients in disaster recovery.

Define: Clearly define the problem and identify key stakeholders.

Ideate: Brainstorm innovative solutions, considering data replication, backup, and failover strategies.

Prototype: Create and test mock-ups or proof-of-concept designs

Test: Conduct real-world testing and gather feedback for refinement.

Implement: Develop and deploy the chosen disaster recovery solutions, ensuring integration with IBM's cloud services

Project Objectives

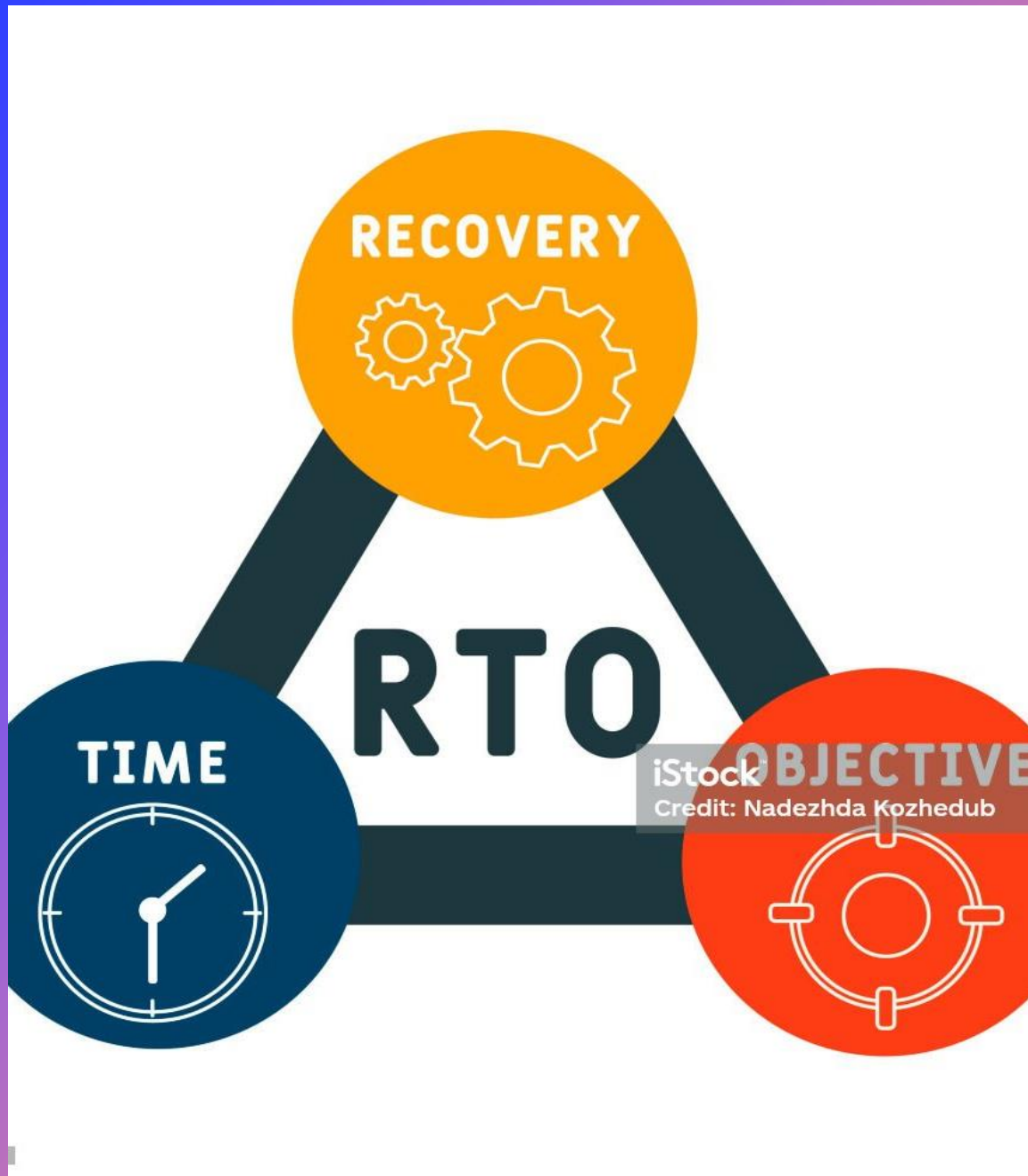
1. High Availability: Ensure that critical services and data remain available and accessible even in the event of a disaster.

2. Data Backup and Recovery: Implement robust data backup and recovery mechanisms to prevent data loss and facilitate the quick restoration of data in case of corruption or failure.

3. Rapid Recovery: Minimize downtime by designing and implementing a disaster recovery solution that enables rapid recovery of systems and data.

4. Testing and Validation: Regularly test and validate your disaster recovery plan to ensure that it works effectively.





Recovery Time Objective:

7

Recovery Time Objective (RTO) is a critical metric in disaster recovery and business continuity planning. It represents the maximum acceptable downtime for a system, application, or service following a disruption. In other words, RTO defines the time within which a system must be restored to avoid significant business impact.

Source Code

```
import time
# Simulate system recovery (replace this with your actual recovery process)
def recover_system():
    print("Recovering the system...")
    time.sleep(5)
# Simulating recovery time (5 seconds in this case)
if __name__ == "__main__":
    start_time = time.time()
    recover_system()
    end_time = time.time()
    recovery_time = end_time - start_time
    print(f"Recovery Time: {recovery_time} seconds")
    # Compare recovery_time to your defined RTO and take appropriate actions defined_rto = 10
    # Replace with your actual RTO
    if recovery_time <= defined_rto:
        print("Recovery within RTO")
    else:
        print("Recovery time exceeded RTO")
```


OUTPUT

Recovering the system...

Recovery Time: 5.0 seconds

Recovery within RTO

Recovery Point Objective:

Crucial metric in disaster recovery and data protection. It represents the maximum tolerable amount of data loss that an organization can accept in the event of a system failure or data disruption. In other words, RPO defines the point in time to which data must be successfully restored after a disruption.



SUMMARY

Disaster recovery in cloud computing is a set of strategies and practices aimed at safeguarding data and applications hosted in the cloud against catastrophic events such as hardware failures, natural disasters, cyberattacks, or human errors. Key elements of cloud-based disaster recovery include data backup, replication, automated failover, and rapid recovery to ensure minimal downtime and data loss. Cloud services offer scalability, redundancy, and cost-effectiveness, making them an attractive option for disaster recovery. Regular testing, security measures, and compliance considerations are vital for a robust disaster recovery plan in the cloud.



+



o



.



THANK YOU