

# Project: Disaster recovery with IBM Cloud virtual servers

## Phase 4: Development Part 2

### Objective:

Continue building the disaster recovery plan by configuring replication and testing recovery procedures using IBM Cloud services.

### Tasks:

#### 1. Replication Setup with IBM Cloud Services:

- Implement replication of data and virtual machine images from on-premises to IBM Cloud Virtual Servers.
- Ensure that data is continually synchronized between on-premises and cloud environments to maintain up-to-date copies.

#### 2. Recovery Testing:

- Conduct recovery tests to ensure that the disaster recovery plan works as intended.
- Simulate disaster scenarios to practice recovery procedures, ensuring that you can minimize downtime and data loss.

### Purpose:

This phase focuses on the technical aspects of disaster recovery. Replication setup ensures data availability in the cloud, and recovery testing validates that the plan functions correctly. It is crucial for achieving the desired RTO and RPO objectives.

In this phase, you are moving from the planning and initial implementation in Phase 3 to the critical aspects of replication and testing in preparation for the actual disaster recovery process.

Certainly, let's delve into more detail about replication setup and recovery testing:

# Replication Setup:

## Definition:

Replication setup is the process of creating and maintaining duplicate copies of data and virtual machine images in a secondary location, often in the cloud. It ensures data redundancy and availability in case of a disaster.

## IBM Cloud's Role:

Utilize IBM Cloud services for replication setup, including custom migration services, to facilitate the continuous and secure transfer of data from on-premises systems to cloud-based virtual servers.

## Continuous Synchronization:

Replication is an ongoing process that ensures data is continually synchronized between the primary (on-premises) and secondary (cloud) environments. This real-time or near-real-time synchronization minimizes data loss and supports your defined RPO.

## Key Steps:

### 1. Data Replication:

Implement continuous replication of data and virtual machine images from your on-premises infrastructure to IBM Cloud Virtual Servers.

### 2. Real-Time Synchronization:

Ensure data synchronization in real-time or near-real-time to minimize data loss and maintain data consistency between the primary and secondary environments.

## Benefits:

Replication setup with IBM Cloud ensures that your data is readily available in a secure off-site location, reducing the risk of data loss during a disaster. This is essential for meeting your business's RPO and achieving data consistency in your recovery process.

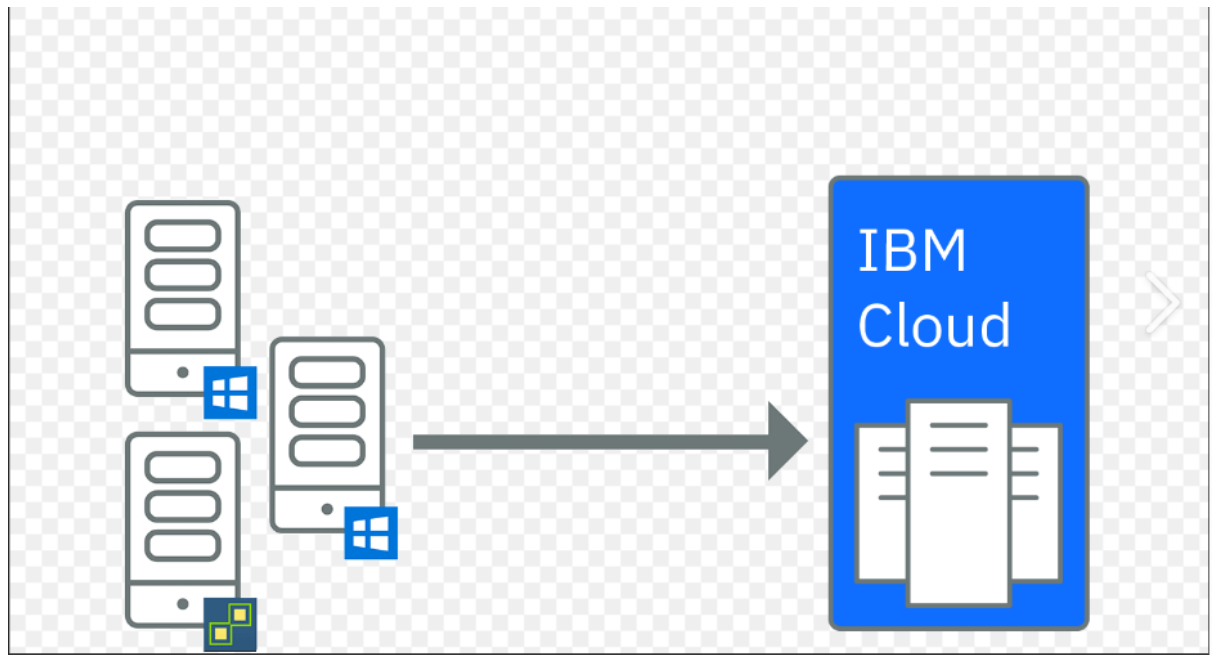


Figure 1 : Data replication in IBM cloud

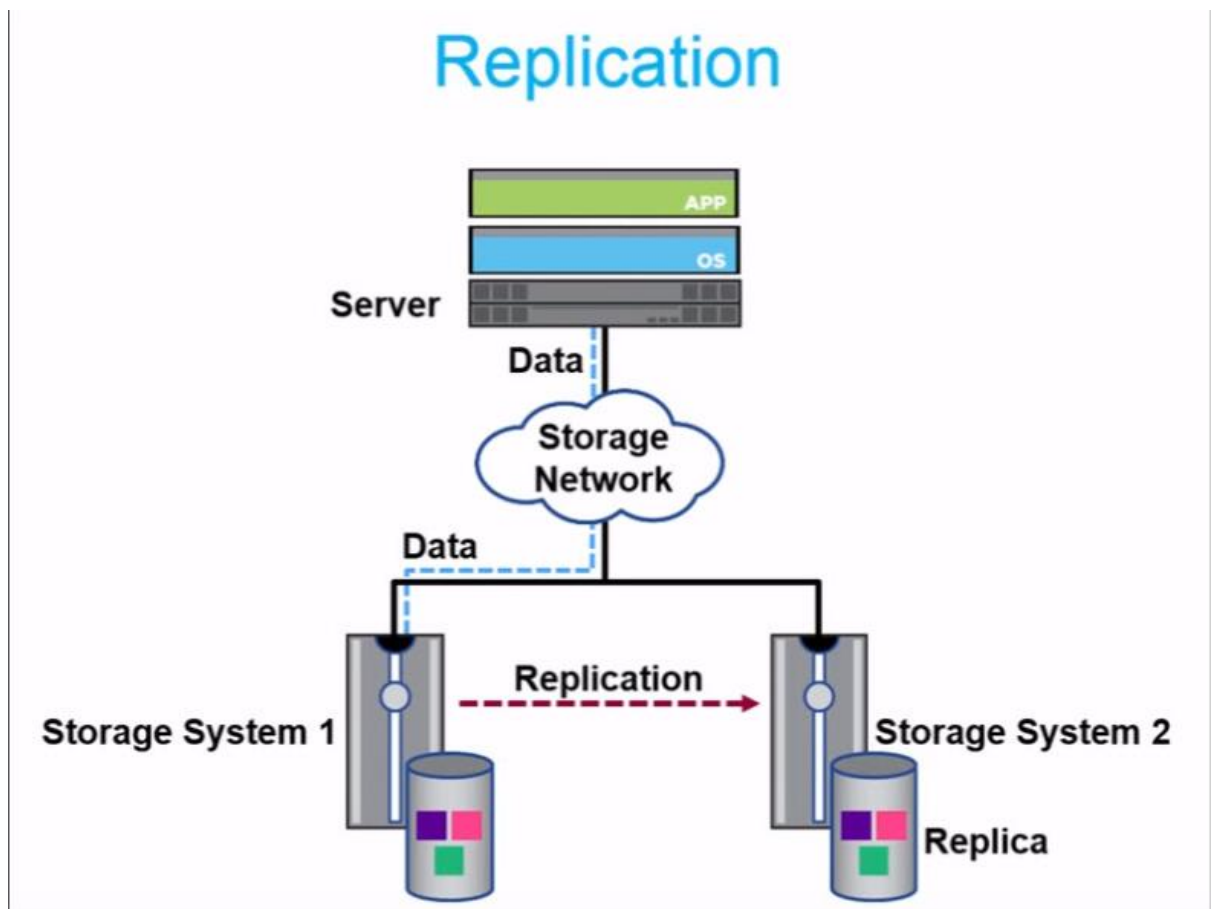


Figure 2 : Replication

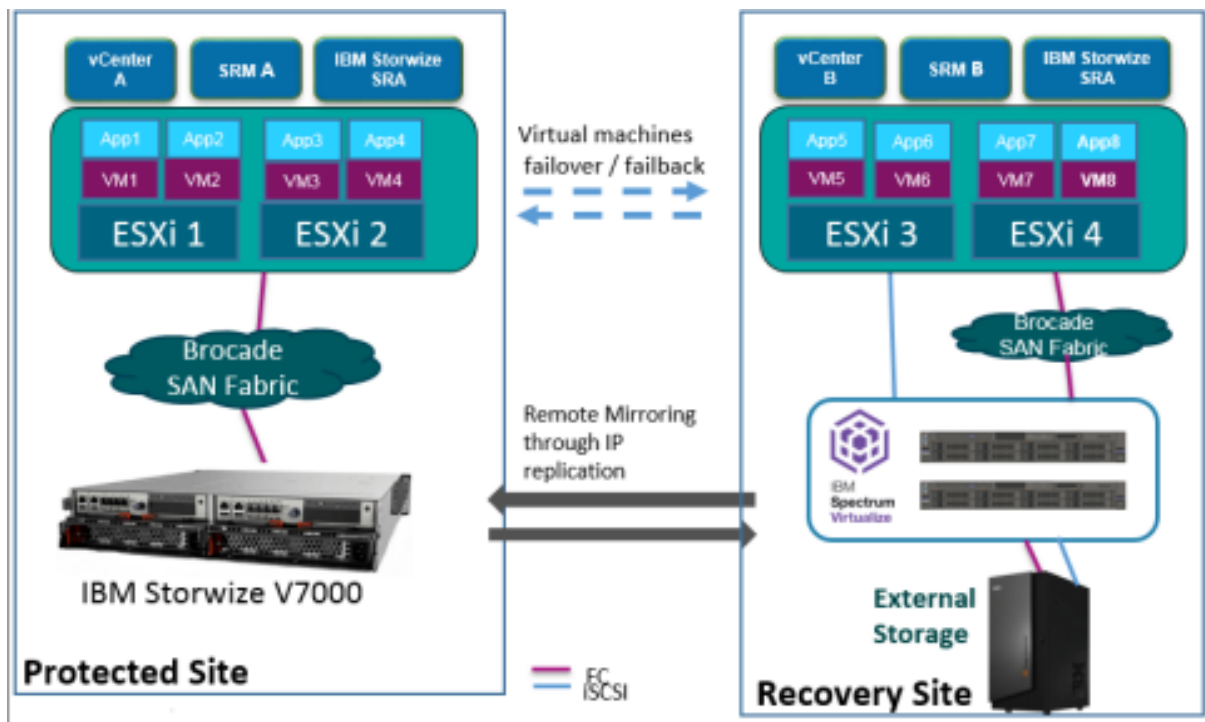


Figure 3 : Lab for Disaster Recovery as service

**VMware vCenter Site Recovery Manager**

**vSphere Platform Services Controller**

Register Site Recovery Manager with a vSphere Platform Services Controller

Provide the Platform Services Controller address.

Address:

HTTPS Port:

vCenter Single Sign-On administrative credentials are required to perform administrative operations in this Platform Services Controller.

Username:  (case-sensitive)

Password:  (case-sensitive)

NOTE: If prompted, you must accept the certificate for the installation to proceed.

InstallShield

< Back   Next >   Cancel

Figure 4 : Recovery manager in Virtual Machine centre

## Recovery Testing:

### Definition:

Recovery testing involves simulating disaster scenarios and executing recovery procedures to ensure that the disaster recovery plan works as intended.

### IBM Cloud's Role:

Incorporate Disaster Recovery as a Service (Disaster Recovery as service) from IBM Cloud to streamline and automate the recovery testing process. Disaster Recovery as service can help simplify the testing procedures and validate the effectiveness of your disaster recovery plan.

## Disaster recovery testing

Last updated 2023-07-31

Disaster recovery (DR) testing is what you must do to keep your ability to be resilient, hoping not to need to do it for real. There are different types of disaster recovery testing that you can do to verify your resiliency capabilities:

- DR dry test
- DR simulation
- Switch-over

## Disaster recovery dry test

A DR dry test is performed by checking all of the resource availability and runbooks on paper, without running a real DR simulation or switch-over.

This type of testing is normally run with higher frequency compared to the other testing flavors as no real activities are performed, but it does require the same effort in terms of skills and people.

The adoption of a recovery orchestrator software improves the whole dry testing process and reduces the time and effort to be run because most of the operations are performed by the software itself. This also increases the preparedness checking of a real DR simulation or switch-over by periodic scanning that all of the components of the DR solutions are in place and works as expected.

## Disaster recovery simulation

DR simulation is a way to verify or audit the emergency runbooks and check the recovery time objectives (RTO) and recovery point objectives (RPO) provided by the solution by simulating as much as possible in the same conditions as a real emergency.

This means introducing disruptions on replication network connections before interrupting the communications among the sites, hence simulating the sudden loss of the primary site.

You can do this only if your data replication solution is resilient and not providing impact on the production, which continues on the primary site. If this is not the case, then look at the documentation for [plan and design for the worst conditions](#).

DR simulation deploys a duplicate of your production environment on the DR site that you can use to perform validation and checking. This environment is cleaned at the end of the simulation and updates that happened to the DR test environment are discarded, as the real production has continued on the primary site.

It is important thus that network streams flowing to the DR test environment are copies of the real production environment. Usually these network flows are intercepted and duplicated at the primary site (that receives the real flow) and sent to the DR site, which operates on separated and different network subnets than production.

## Switch-over

Opposite to the DR simulation, in the switch-over test, production is moved from primary site to DR site to verify and audit the ability to run and sustain production operations for a long period.

In this option, we don't test DR runbooks, as this would imply the emergency restart, which has an impact on the production environment.

To avoid any impact to the production environment, you should pose all the possible attention in performing this switch, such to minimize all those impacts.

Production operations are closed orderly on the primary site and reopened from the DR site.

Data replication is reverted once everything in the DR site has been verified and before network streams are rerouted to the DR site.

Production runs in the DR site for whatever period you have chosen before returning to the primary site at your most convenient time. During this period, your production site is performing as the DR until the next switch-over.

Updates happened to the production running in the DR site is kept and replicated back to the primary site.

## Testing Scenarios:

Create a range of disaster scenarios, such as hardware failures, data corruption, or site outages, and then execute the recovery procedures outlined in your plan.

## Validation:

The primary objective of recovery testing is to verify that the recovery plan can achieve your defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Testing helps ensure minimal downtime and data loss during an actual disaster.

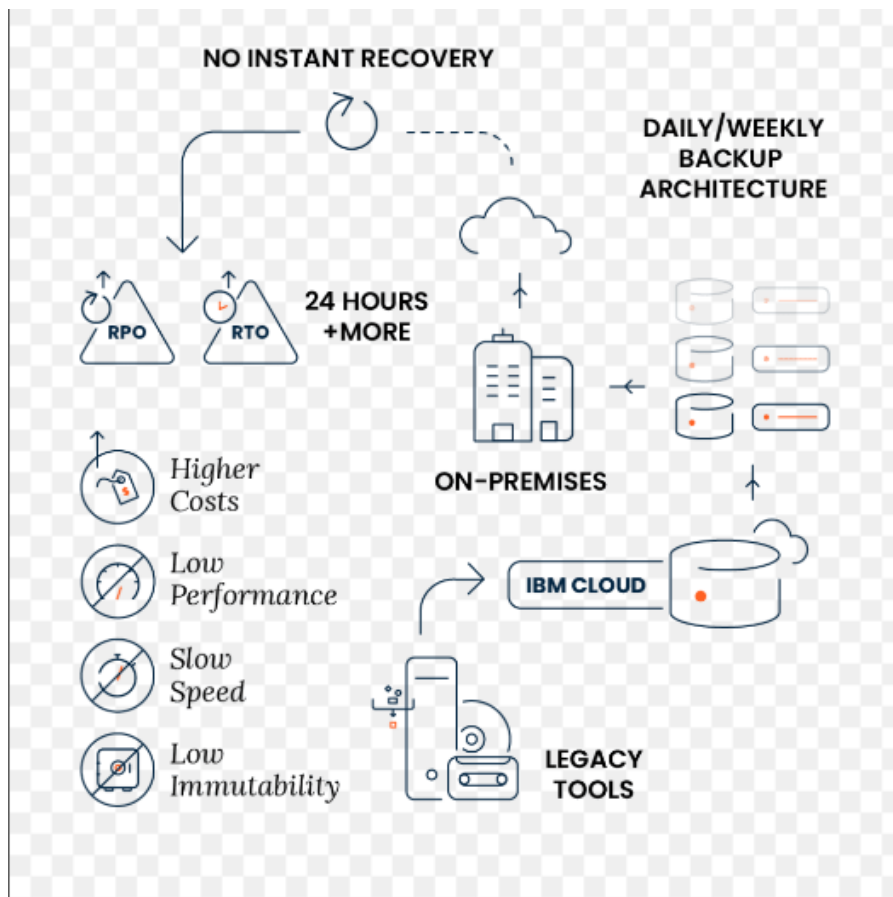
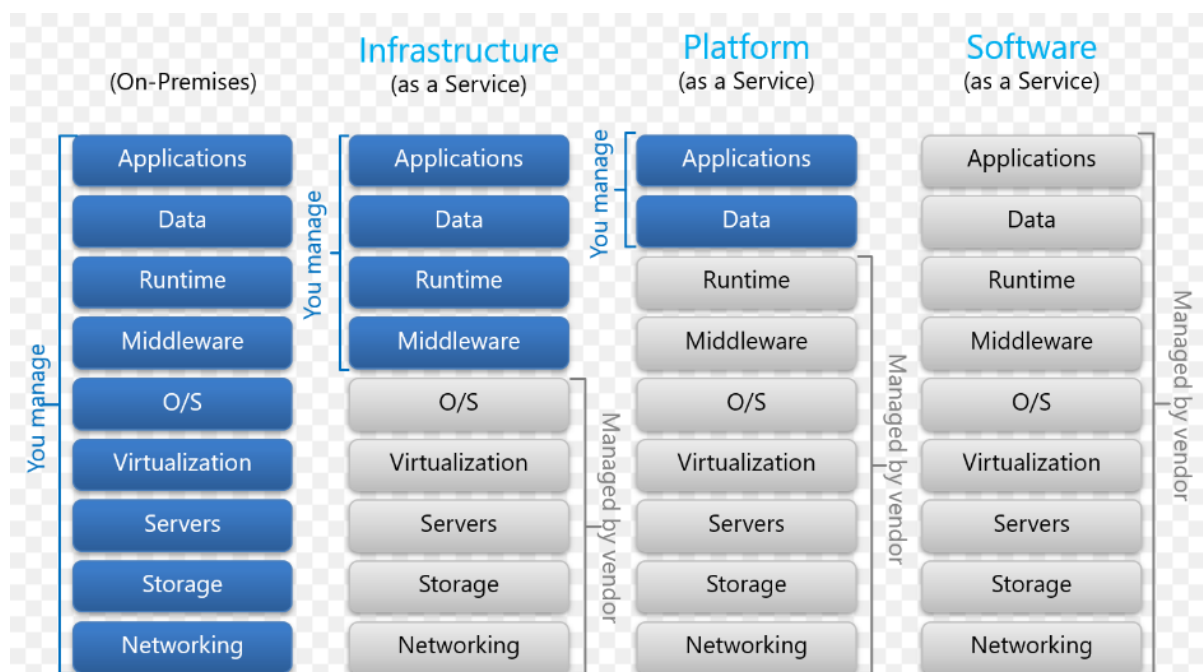
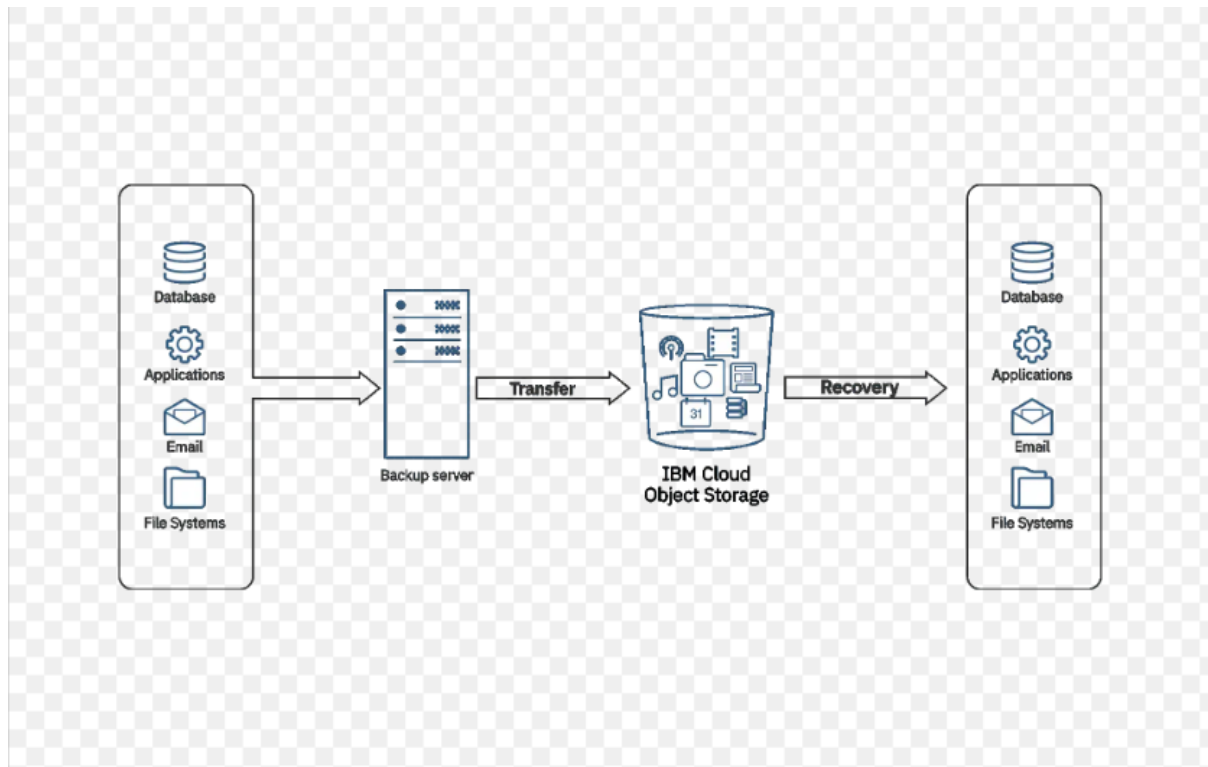


Figure 5 : This type is not suitable







*Figure 6 : Backup method in IBM Cloud*

## Key Steps:

### 1. Scenario Creation:

Develop various disaster scenarios, such as hardware failures, data corruption, or site outages, to simulate potential real-world disruptions.

### 2. Testing Execution:

Execute the recovery procedures outlined in your disaster recovery plan for each scenario to verify that they can achieve your defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

### 3. Validation:

Recovery testing helps identify any weaknesses in your plan and provides an opportunity to fine-tune it for optimal performance

## Benefits:

Recovery testing is crucial for identifying any weaknesses in your disaster recovery plan and fine-tuning it to meet your business continuity goals. With IBM Cloud's Disaster Recovery as a Service, you can efficiently conduct these tests and gain confidence in your recovery procedures.

Both replication setup and recovery testing are pivotal components of your disaster recovery strategy. Replication ensures data availability, while recovery testing validates the plan's effectiveness in achieving your RTO and RPO objectives, ultimately guaranteeing business continuity in the face of unforeseen events.