DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

PROJECT OVERVIEW :

The project titled 'Disaster Recovery with IBM Cloud Virtual Servers' aims to establish a robust and reliable disaster recovery solution utilizing IBM Cloud's virtual server infrastructure. This project's primary goal is to ensure the continuity of critical business operations in the face of unexpected disruptions, such as natural disasters or hardware failures. Key components include data replication, failover mechanisms, and automated recovery processes, all leveraging IBM Cloud's scalable and secure virtual server environment. By implementing this disaster recovery strategy, organizations can minimize downtime, protect valuable data, and maintain business resilience in the event of unforeseen crises. Project Objectives

DEFINITION:

Disaster recovery (DR) is a crucial aspect of any business continuity plan, and it involves ensuring the rapid recovery of IT systems and data in the event of a disaster or disruptive event. IBM Cloud provides a range of services, including virtual servers, that can be leveraged for disaster recovery purposes.

SOFTWARE COMPONENTS:

IBM offers several software components and services that can be used for disaster recovery in their cloud servers. Here are some key components and services:

THEY ARE :

1. **IBM Resiliency Orchestration:** This software helps automate disaster recovery processes and can work with various cloud environments. It enables you to define and execute recovery plans.
2. **IBM Cloud Virtual Servers:** You can use IBM Cloud's virtual servers to host your applications and data. These can be configured in a way that allows for backup and replication, which is a fundamental aspect of disaster recovery.
3. **IBM Cloud Object Storage:** This service provides scalable, durable, and highly available storage for your data. It can be used to store backups and ensure data resiliency.
4. **IBM Cloud Backup:** This service provides backup and recovery capabilities for cloud resources, including virtual servers and cloud databases.
5. **IBM Cloud Resilience:** This is a Disaster Recovery as a Service (DRaaS) solution provided by IBM. It offers automated, continuous replication of data to a secondary site for recovery in the event of a disaster.
6. **IBM Cloud Monitoring with Sysdig:** Monitoring your cloud resources is critical for disaster recovery. IBM offers monitoring solutions that help you track the health and performance of your applications and infrastructure.
7. **IBM Cloud Internet Services:** Content Delivery Network (CDN) and DDoS protection services can be essential for ensuring that your applications remain accessible during and after a disaster.

RTO'S AND RPO'S OF DISASTER RECOVERY:

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are two key metrics in disaster recovery planning. They help organizations define and measure their goals for recovering from a disaster or disruption.

1. **Recovery Time Objective (RTO):**

   - **Definition:** RTO is the maximum acceptable time it should take to restore a system or service after a disruption or disaster.
   - **Importance:** RTO helps in determining how quickly a business process or IT service needs to be restored to avoid significant harm to the business.
   - **IBM Cloud Virtual Servers and RTO:** The RTO for disaster recovery using IBM Cloud Virtual Servers would depend on various factors, including the complexity of your infrastructure, the nature of the disaster, and the efficiency of your recovery processes. IBM Cloud provides features such as virtual machine snapshots, backup services, and automation tools that can contribute to minimizing RTO.

2. **Recovery Point Objective (RPO):**

   - **Definition:** RPO is the maximum acceptable amount of data loss measured in time. It signifies the point in time to which data must be recovered after a disruption.
   - **Importance:** RPO helps in determining the maximum tolerable data loss for specific business processes or IT services.
   - **IBM Cloud Virtual Servers and RPO:** The RPO in a disaster recovery scenario using IBM Cloud Virtual Servers depends on your backup and data replication strategies. IBM Cloud offers various tools and services for data backup, including block storage snapshots, object storage, and database backup solutions. Leveraging these tools and ensuring regular backups can contribute to minimizing data loss and achieving a lower RPO.

   In summary, when implementing disaster recovery using IBM Cloud Virtual Servers:

- To minimize RTO, utilize automation tools, and have well-defined recovery procedures. IBM Cloud provides features to help automate the deployment of virtual machines and applications.
- To minimize RPO, implement robust backup and data replication strategies using IBM Cloud's storage and backup services.

STRATEGIES FOR DISASTER RECOVERY:

Disaster recovery strategies using IBM Cloud Virtual Servers involve planning and implementing measures to ensure the availability and continuity of critical systems and data in the event of a disaster or disruptive event. Here are some key strategies:

1. Backup and restore
2. Replication
3. High Availability(HA)
4. Automated Deployment and Orchestration
5. Site Recovery manager
6. Testing and validation’
7. Security Measures
8. Documentation and Training
9. Monitoring and Alerts
10. Collaboration with IBM support

PRIORITIES OF VIRTUAL MACHINE:

- Performance
- Resource Isolation
- Security
- Availability and Redundancy
- Scalability

- Backup and Disaster Recovery
- Networking
- Resource Monitoring and Management
- Compliance
- Cost Optimization
- Integration with Management tools
- User experience
- Licensing and software compliance

GENERAL STEPS:

1. **Identify crucial workloads:**
   Identify the virtual servers and workloads that are critical for your business operations. Classify these workloads based on their importance and the level of recovery priority.

2. **Backup and replication :**
   Use backup and replication tools to create copies of your virtual server data. IBM Cloud offers services like IBM Cloud Object Storage for scalable and durable storage of backup data.

3. **Replication to a secondary location:**
   Set up replication of virtual server data to a secondary location, preferably in a different geographical region to mitigate regional disasters. IBM Cloud offers services like IBM Cloud Virtual Servers for VPC that can be deployed in different regions.

4. **Use cloud object storage:**
   Leverage IBM cloud object storage for storing backup data. This provides scalable, durable andhighly available storage for your backups.

5.Automate disaster recovery processes:

Automate the disaster recovery processes to minimize downtime. This may involve scripting and utilizing automation tools available on the IBM Cloud platform.

6.Create recovery plans:

Develop detailed recovery plans that outline the steps to be taken in the event of a disaster. Ensure that these plans are regularly tested to verify their effectiveness.

7.Utilize IBM cloud services :

Take advantage of specific IBM Cloud services designed for disaster recovery, such as IBM Resiliency Orchestration.

8.Network configuration :

Set up networking configurations that facilitate failover to the secondary location. Use IBM Cloud's Virtual Private Network (VPN) or Direct Link services for secure communication between primary and secondary environments.

9.Monitoring and Alerts :

Implement monitoring tools to keep track of the health and performance of your virtual servers. Configure alerts to notify administrators of any issues that may impact disaster recovery.

10.Regular testing :

Regularly test your disaster recovery plans to ensure they work as expected. Conduct simulated disaster recovery drills to assess the efficiency and effectiveness of your recovery processes.

DISASTER RECOVERY STEPS:

STEP 1 :

Use a Terraform to define and provision virtual servers on IBM cloud. Create a Terraform configuration file . (eg. “main.tf”) with your server configurations.

CODE :

```
 provider "ibm" {
// Configure IBM Cloud provider details
}
resource "ibm_compute_instance" "primary_instance" {
 // Define primary server details
 }
resource "ibm_compute_instance" "dr_instance" {
// Define disaster recovery server details
}
```

Configuration :

```
terraform init
terraform apply
```

STEP 2 : configure data replication

set up data replication between the primary and disaster recovery servers. This can be achieved using various tools such as storage replication or database replication, depending on your application architecture

STEP 3: Automate backup and restore scripts :

Create scripts to automate the backup and restore processes. These scripts should be capable of taking regular backups of your data from the primary server and restoring it to the disaster recovery server.

CODE :

```
# backup.sh

tar -czvf /path/to/backup.tar.gz /path/to/data


# restore.sh

tar -xzvf /path/to/backup.tar.gz -C /path/to/dr-server
```

STEP 4 : Automate failover process :

implement a failover script that switches your application traffic from the primary server to the disaster recovery server in case of a disaster. This script might involve updating DNS records, adjusting load balancer settings, or reconfiguring network settings.

CODE :

```
# failover.sh

# Update DNS records or load balancer settings to redirect traffic to the DR sever .
```

STEP 5 : Test the disaster recovery process:

Regularly test your disaster recovery process to ensure that it works as expected. This involves simulating a disaster and validating that the failover and recovery processes function correctly.