**GROUP 5**

*Project on*

**Disaster Recovery with IBM Cloud Virtual Servers**

**PRESENTED BY,**

**Malavika M.S**

**Mercia Carool S.A**

**Midhuna M.B**

**Petrishiya Golgy S**

**Safana Jesrin M**

**PROBLEM STATEMENT**

Safeguard business operations with IBM Cloud Virtual Servers. Create a disaster recovery plan for an on-premises virtual machine, ensuring continuity in unforeseen events. Test and validate the recovery process to guarantee minimal downtime. Become the guardian of business continuity, securing the future of your organization!

**SOLUTION**

To create a disaster recovery plan for an IBM cloud virtual server, you can set up replication for your server's data to a secondary location. This ensures that if a disaster occurs, you can quickly recover your server and data.

**OBJECTIVES**

* + Identify critical VM
  + Choose IBM cloud virtual Servers
  + Establish data backup and replications
  + Develop a plan
  + Test the plan
  + Automate where possible
  + Document the recovery team
  + Monitor and update the plan
  + Secure the data

**DISASTER RECOVERY STRATEGY**

It is a plan that helps protect your important applications and data in case of unexpected events.

* + Identify important data
  + Choose a backup solution
  + Set up replication
  + Test the plan regularly
  + Document and train the team

**BACKUP CONFIGURATION**

It refers to the process of setting up and managing backups for your data and applications.

* + Data needs to be backed up
  + Select the appropriate backup solution
  + Configure the setting

**REPLICATION SETUP**

It involves configuring the replication of data between multiple locations or instances to ensure redundancy and data availability.

* + Use services like IBM cloud database

**RECOVERY TESTING**

It involves testing the effectiveness of your disaster recovery plan to ensure that your applications and data can be successfully recovered ina case of failure.

* + Identify the critical applications and data
  + Set up a separate environment
  + Restore the necessary data
  + Validate the functionality
  + Monitor and access
  + Document

**BUSINESS CONTINUITY**

It refers to the strategies and practices put in place to ensure the continuous operation.

* + High availability
  + Disaster recovery
  + Backup and restore
  + Monitoring and alerting
  + Security

**TRADITIONAL DISASTER RECOVERY**

* **No offsite data**

It is a backup process, where we can secure data in the event of disaster. That means documents recovery might takes weeks besides can be unsuccessful.

* **Backup with no host site**

It refers the data is backed up by offsite (data are stored in a separate physical location) but not hot site (duplicate of the main site). To get the data that is stored would take time.

* **Data backup with hot site**

It means every association should preserve data standby servers as well as hot site. This hot site backup determination results in the requirement to re-form some hours or days to recover information, but recovery period can be anticipated.

* **Electronic vaulting**

It is an alternative of backup physically like tapes it offers technique called electronic vaulting, files are backed up and electrically transmitted to a secure storage location contains high-speed circuit communication, a few frame of channel expansion hardware and remote sites.

* **Point in time copies**

This type of solutions requires larger information exchange and quicker recovery than clients of inferior tiers. PIT means every association preserves and uses appropriate this holdup of critical information which is web reachable to backup site.

* **Transaction integrity**

The businesses that use this type of solutions are consistency of data between the production data sites and the recovery data sites. Such that any records damage can be done.

* **Zero or near data loss**

BCP maintains the data concurrency industries by means of slight or no allowance intended for information loss and wants to bring back information to tenders in a fast way. It doesn’t depend on the applications to provide data consistency.

* **Highly automated, business integrated solution**

It ensures consistency of data that which is agreed by minimal data loss solutions. It also provides the recovery of the appliance which is computerized and allows for renewal of systems such that application becomes fast and consistent.

**DISASTER RECOVERY STRATEGY**

* **Backup Configuration**

It refers to the process of setting up and managing backups for your data and applications

* Data needs to be backed up
* Select the appropriate backup solution
* Configure the setting
* **Replication Setup**

It involves configuring the replication of data between multiple locations or instances to ensure redundancy and data availability

* Use services like IBM cloud database
* **Recovery Testing**

It involves testing the effectiveness of your disaster recovery plan to ensure that your applications and data can be successfully recovered in a case of failure

* Identify the critical applications and data
* Set up a separate environment
* Restore the necessary data
* Validate the functionality
* Monitor and access
* Document
* **Business Continuity**

It refers to the strategies and practices put in place to ensure the continuous operation

* High availability
* Disaster recovery
* Backup and restore
* Monitoring and alerting
* Security

**INNOVATION IN DISASTER RECOVERY**

**1. Identify critical data and applications:**

Determine which data and applications are essential for your business operations.

**2. Assess risks:**

Evaluate potential risks and threats that could impact your virtual server, such as hardware failures, natural disasters, or cyberattacks

**3. Define recovery objectives:**

Set recovery time objectives (RTO) and recovery point objectives (RPO) to determine how quickly you need to recover your server and how much data loss is acceptable.

**4. Develop a recovery strategy:**

Create a plan outlining the steps and procedures to recover your virtual server in case of a disaster. This may include backup and replication strategies, failover mechanisms, and testing procedures.

**5. Implement backup and replication solutions:**

Set up regular backups and implement replication mechanisms to ensure data redundancy and availability.

**6. Test the plan:**

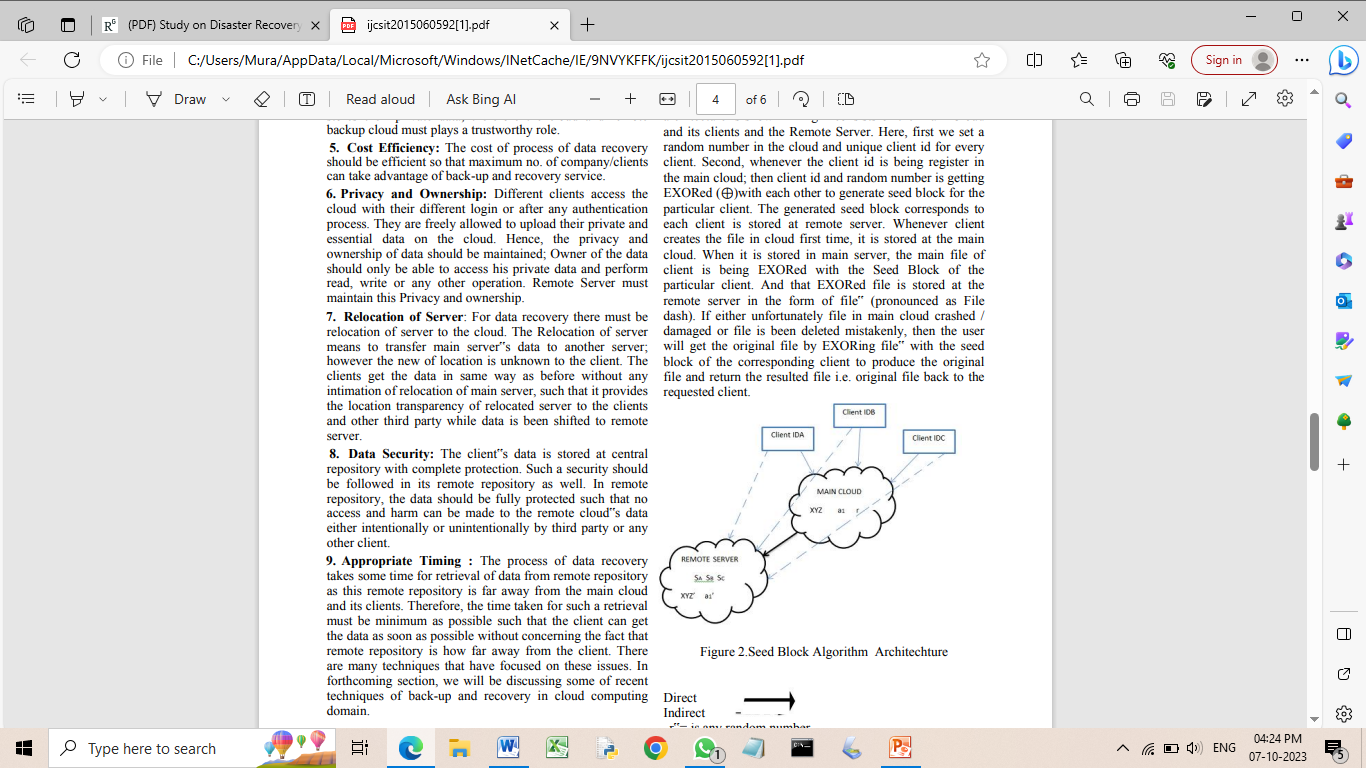
Regularly test your disaster recovery plan to identify any weaknesses or gaps. This will help ensure that your plan is effective and can be executed smoothly when needed.

**7. Document and update:**

Document your disaster recovery plan and keep it up to date with any changes to your virtual server environment or business requirements.

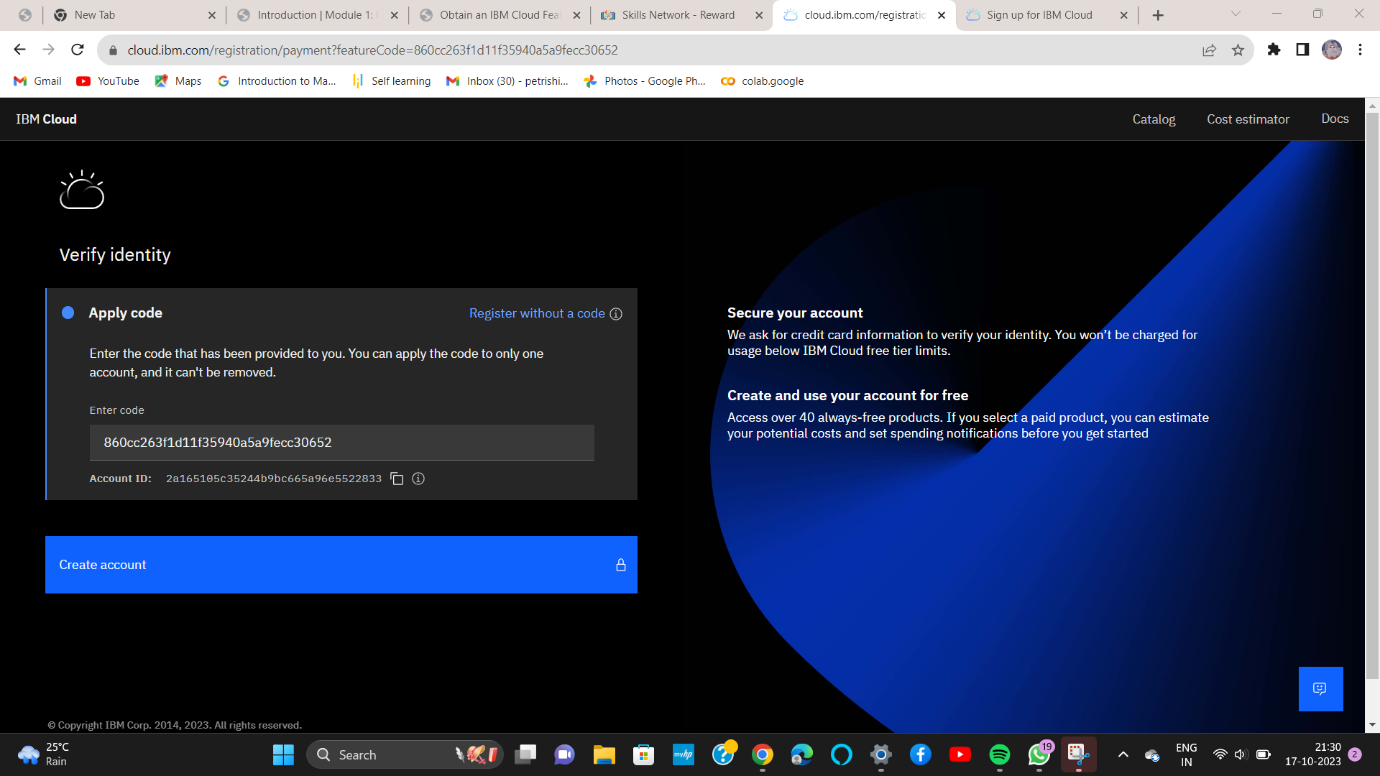
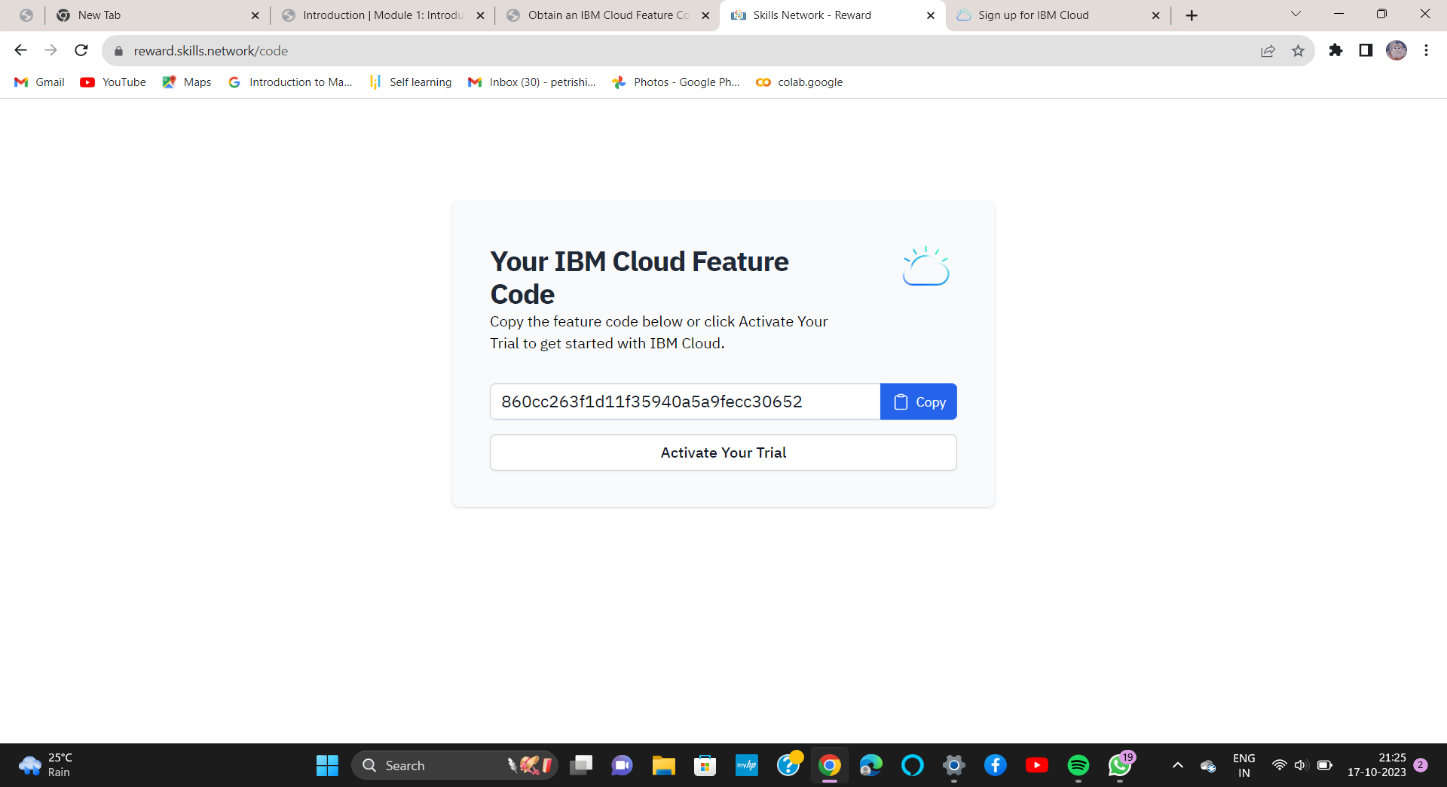
**SEEDBLOCK ALGORITHM**

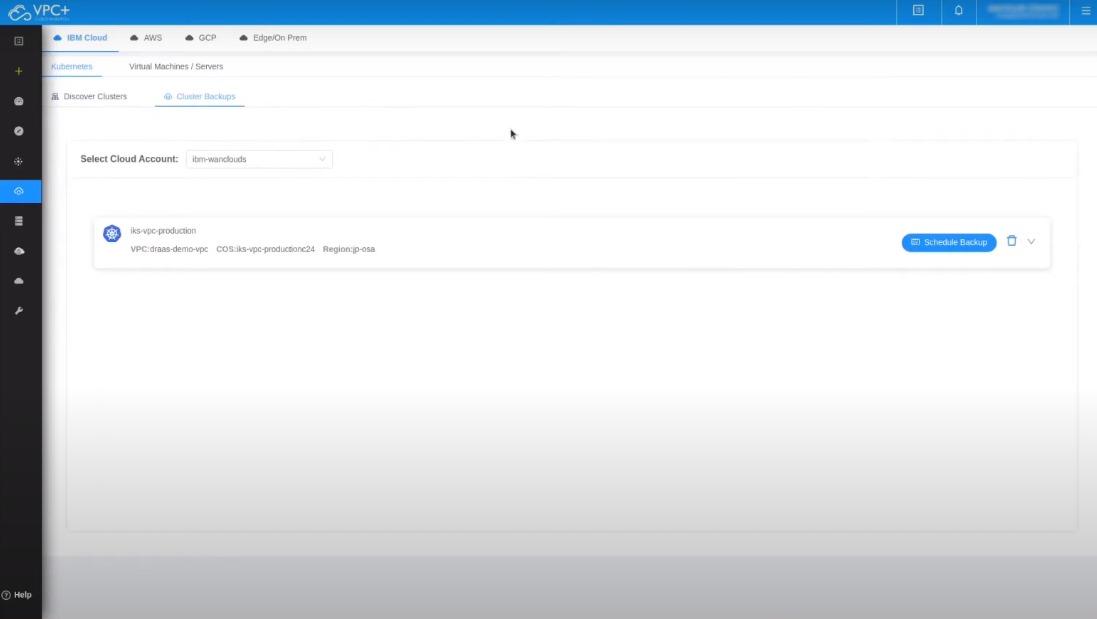
The SeedBlock algorithm is used for data encryption and decryption. It is a cryptographic algorithm that uses a combination of a seed value and a block cipher to securely encrypt and decrypt data. This algorithm is commonly used in applications that require data protection and confidentiality, such as secure communication channels and storage systems.

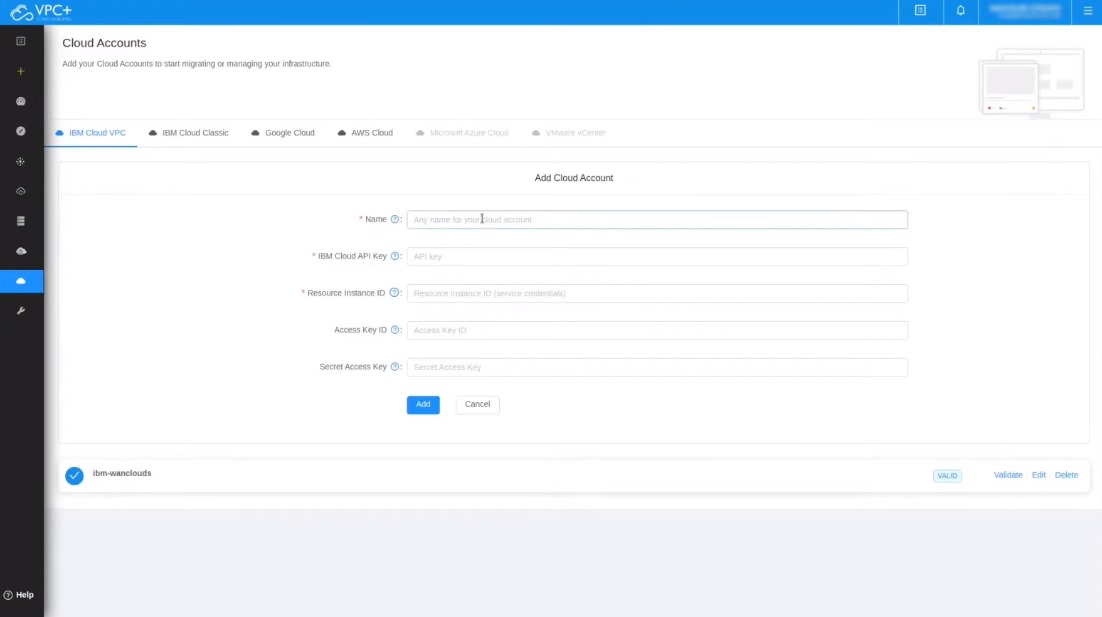


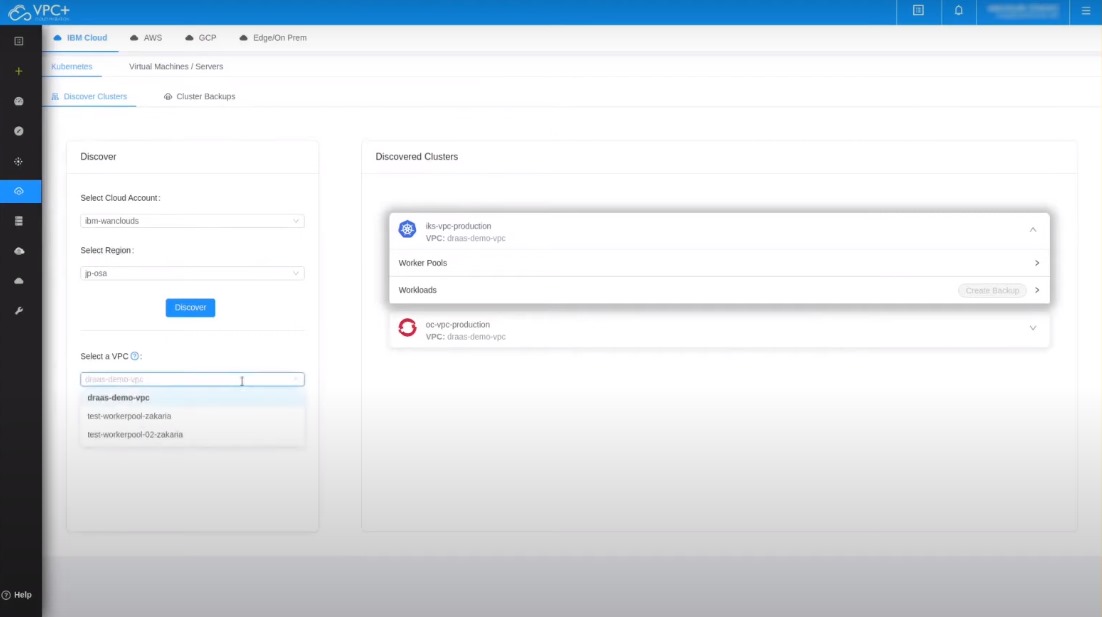
**DEVELOPMENT STEPS**

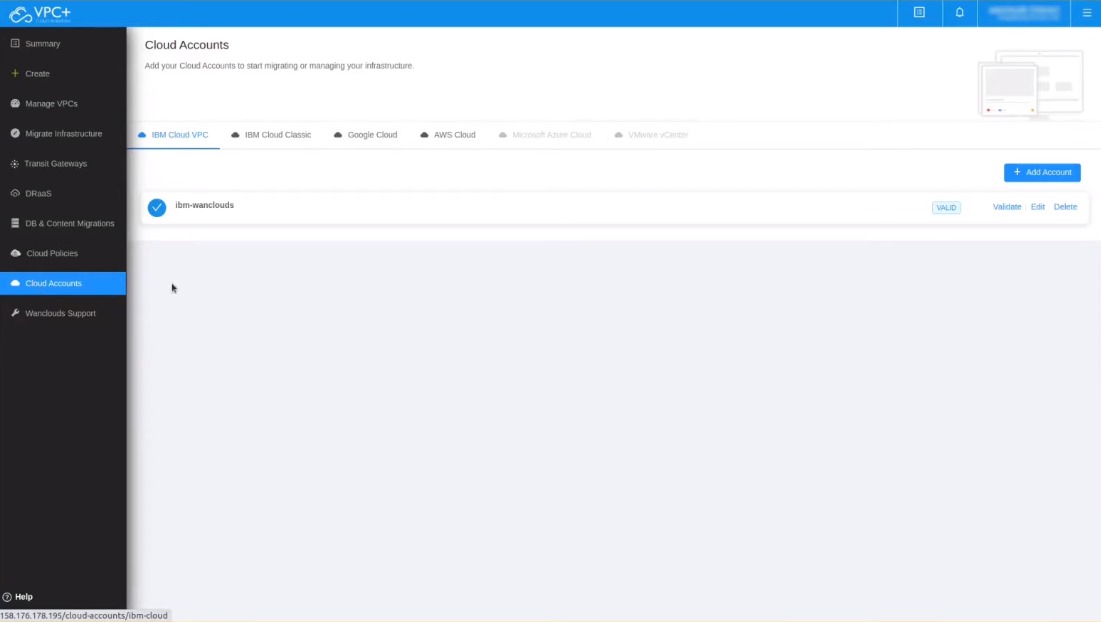
This project is done using IBM Cloud Foundry.

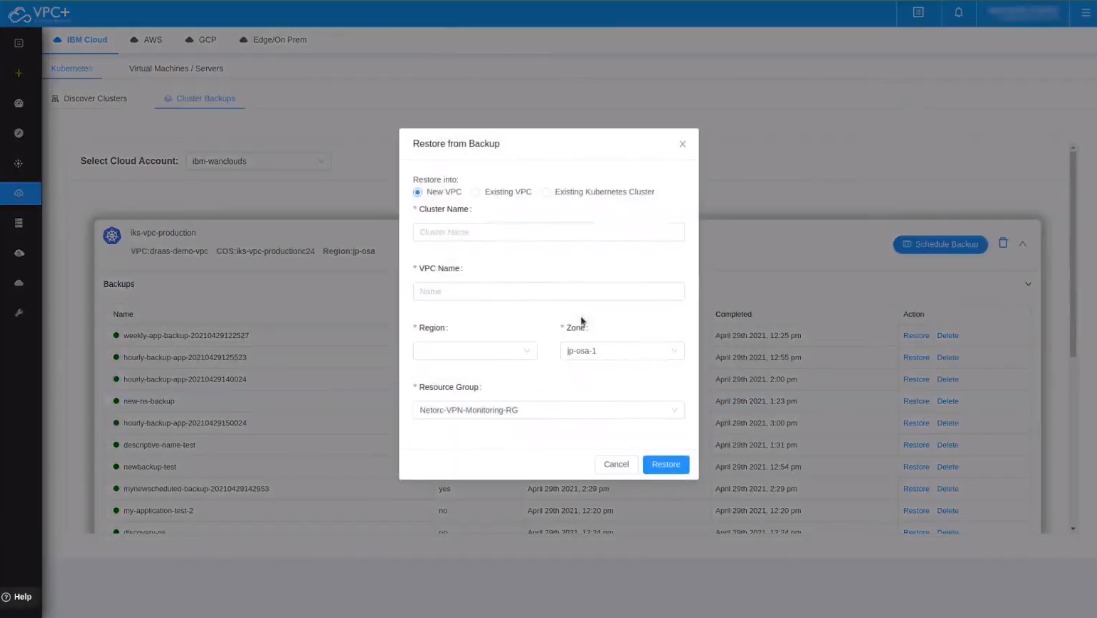


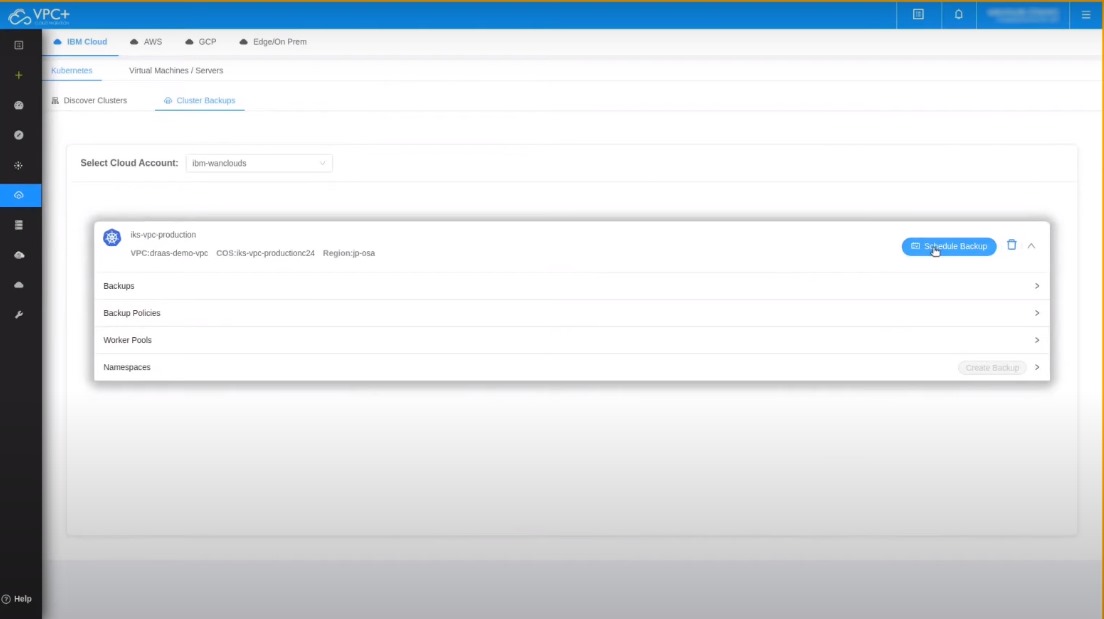


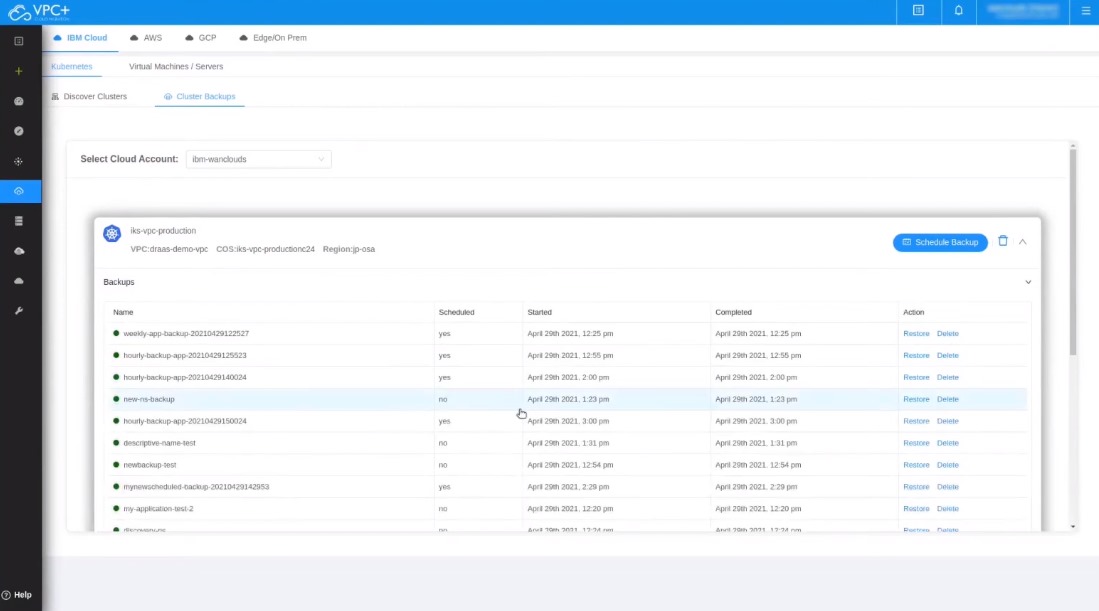


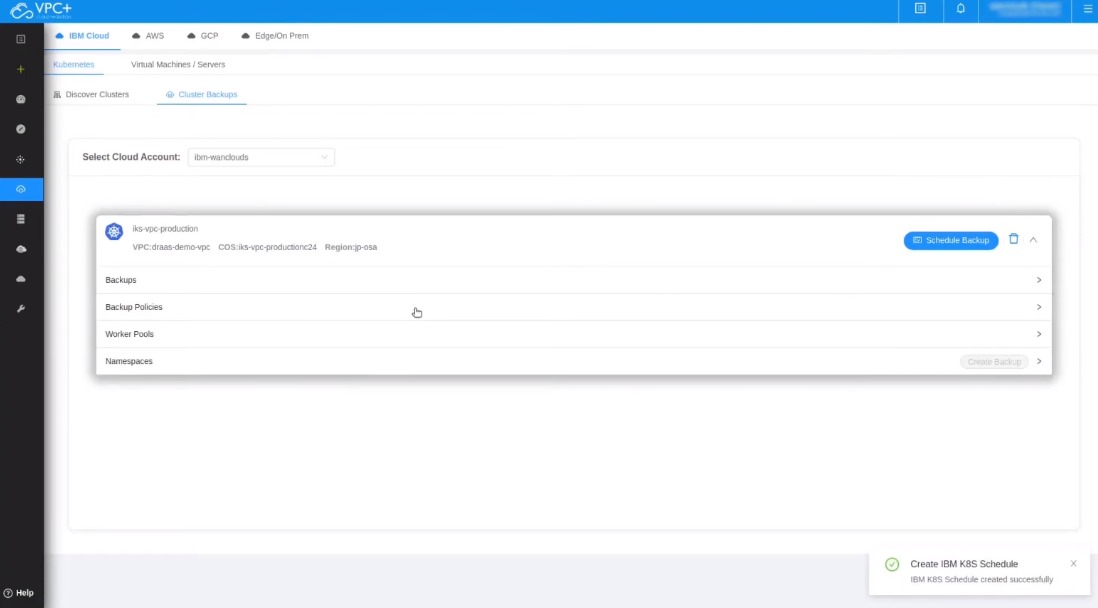


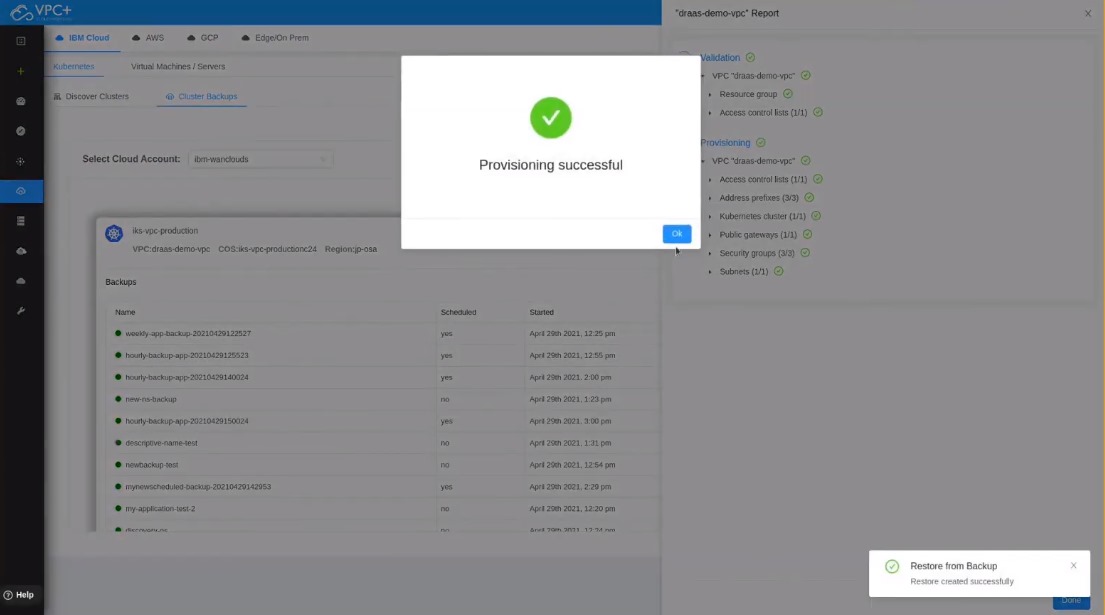
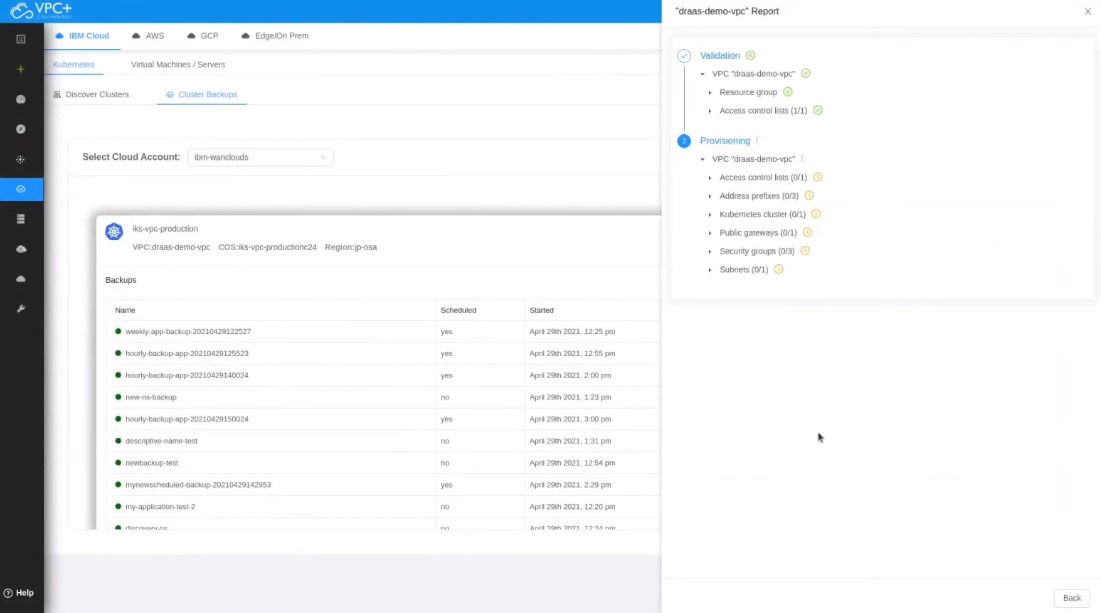


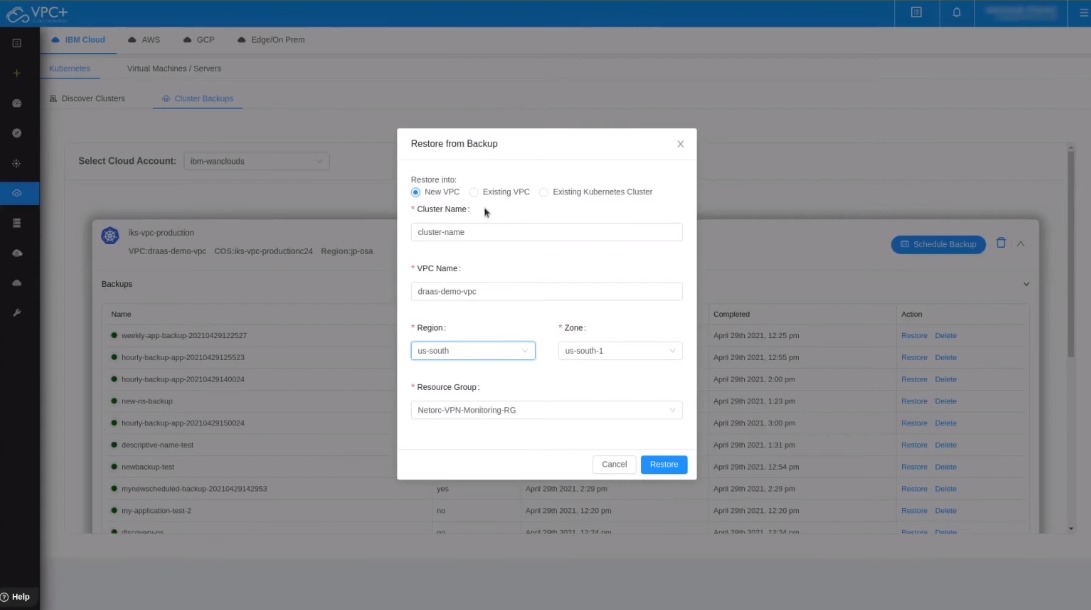


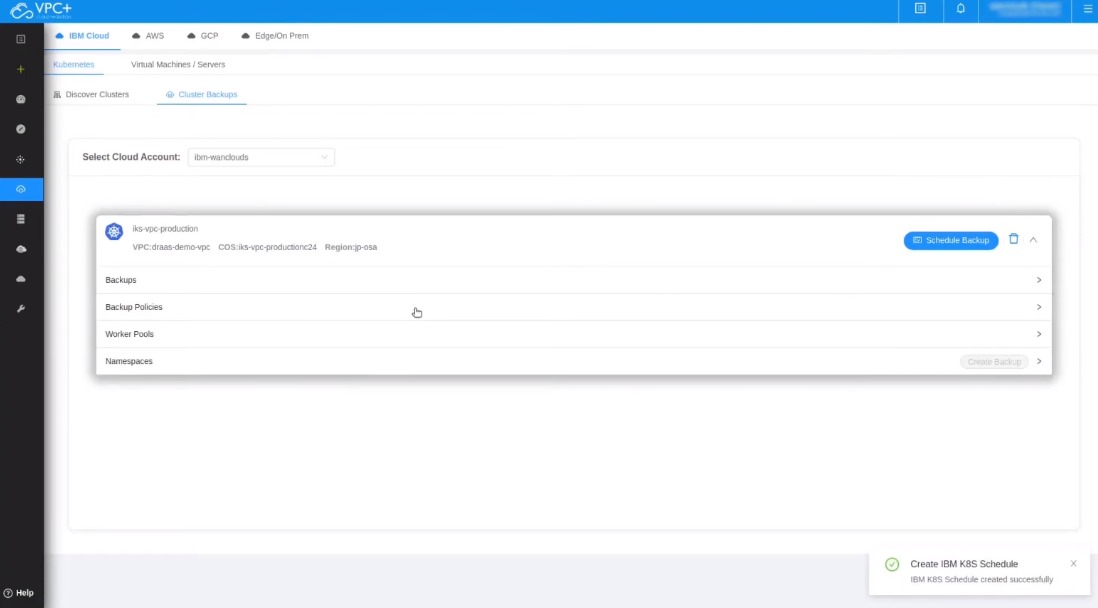












**CONCLUSION**

In conclusion, disaster recovery with IBM Cloud provides robust solutions to ensure the continuity of your business operations. With features like high availability, disaster recovery options, backup and restore capabilities, monitoring tools, and strong security measures, IBM Cloud offers a comprehensive platform to protect your data and applications from disruptions.