|  |  |
| --- | --- |
| **Date** | **01-11-2023** |
| **Team ID** | **4154** |
| **Project Name** | **Disaster Recovery with IBM Cloud Virtual Servers** |

**PROJECT DOCUMENTATION AND SUBMISSION**

**Table of content:**

|  |  |
| --- | --- |
| 1 | Introduction |
| 2 | Problem Statement |
| 3 | Literature Survey |
| 4 | Design thinking process |
| 5 | Disaster recovery strategy |
| 6 | Description of Development phases |
| 7 | Technology architecture |
| 8 | Modules description |
| 9 | Algorithm and Technology used |
| 10 | Project development steps and screenshot |
| 11 | Conclusion |

**Introduction**

The task at hand is to develop a Disaster recovery with IBM using cloud virtual servers is a critical component of ensuring business continuity in the face of unforeseen disruptions. IBM offers robust solutions that leverage cloud technology to safeguard your data and applications.

**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.

**Literature Survey:**

**1. PAPER NAME:** Cloud Computing: A Review Paper

**AUTHOR NAME:** AbhishekGautam

**YEAR:** 2022

**CONTENT:** This is a text about cloud computing, a technology that allows users to access applications and data remotely through the internet. The text discusses the benefits of cloud computing, including cost savings, accessibility, and security. It also explains the different types of cloud computing services, such as SaaS, PaaS, and IaaS. The text highlights the importance of cloud computing in various industries and in personal use. It concludes by discussing the challenges that may arise in the future due to the spread of cloud computing

**2. PAPER NAME:** Disaster recovery in cloud computing

**AUTHOR NAME:** A. Alwan

**YEAR:** 2022

**CONTENT:** It provides an overview of DR and its different types, as well as the current recovery techniques. The paper also examines the challenges of DR mechanisms and the issues concerning data backup and recovery in the cloud paradigm. The authors suggest that an effective and practical DR plan is necessary to maintain financial success and sustain the future growth of an organization. The paper concludes by identifying future directions for DR in cloud computing.

**3. PAPER NAME:** Data Recovery and Back management

**AUTHOR NAME:** Nadeem Sarwar

**YEAR:** 2021

**CONTENT:** This is a paper discussing cloud computing and its benefits for storing data and information online. The paper highlights the importance of having a proper backup plan for data recovery and the need for secure and protected data storage. The paper also discusses different cloud platforms that businesses can use to store critical information and how they handle data backup and recovery. The paper emphasizes the importance of data security and encryption to protect against internet threats. The paper concludes with a discussion of a system prototype setup for practical network applications.

**4. PAPER NAME:** A Secure Backup System

**AUTHOR NAME:** Reda Maher

**YEAR:** 2021

**CONTENT**: The importance of data backup and the threats posed by digital data storage. Cloud backup systems are commonly used to protect against these threats, but there are challenges in ensuring the protection of user data. The paper proposes a system called Drop Store that utilizes the advantages of multi-cloud storage and Fog Computing to ensure users' data protection and reliability. The proposed system has many advantages over existing systems, including fast backup, better user experience, and no dependency on untrusted third parties for security management. The paper also discusses the benefits of multi-cloud architecture for data storage and backup and provides an overview of previous work in Multicolour backup systems and research efforts in Fog Computing-based storage.

**5. PAPER NAME:** An analysis on data recovery and backup technologies in cloud computing

**AUTHOR NAME:** Dhriti Mohan

**YEAR:** 2020

**CONTENT:** Explores various data backup and recovery techniques used in cloud computing. The paper discusses the need for data backup and recovery services due to the large amount of data generated daily and the potential loss of this data. The authors review several papers that propose different backup techniques; including seed block algorithms, semantic-based systems, and signcryption. The advantages and disadvantages of each technique are compared, and the importance of an efficient remote data backup server is emphasized. The paper concludes by summarizing the key points and critical details of each technique.

**Design thinking process:**

Design thinking can also be applied to the deployment and utilization of IBM Cloud Virtual Servers in disaster recovery scenarios. Here's a step-by-step design thinking process for integrating IBM Cloud Virtual Servers into your disaster recovery strategy:

1. Empathize:

- Understand the unique requirements and constraints of your organization's disaster recovery needs.

- Gather insights by speaking with IT professionals, disaster recovery experts, and key stakeholders to identify specific challenges and goals.

2. Define:

- Clearly define the scope of your disaster recovery project, including the critical applications, data, and systems that need to be protected.

- Identify the specific technical requirements and constraints associated with using IBM Cloud Virtual Servers for disaster recovery.

3. Ideate:

- Assemble a cross-functional team that includes cloud experts, IT administrators, and disaster recovery specialists.

- Brainstorm creative solutions for integrating IBM Cloud Virtual Servers into your disaster recovery plan. Consider factors like scalability, reliability, and cost-effectiveness.

4. Prototype:

- Create prototypes or proofs of concept to demonstrate how IBM Cloud Virtual Servers can be used for disaster recovery.

- Develop templates for virtual server configurations, network setups, and data replication processes.

5. Test:

- Implement the prototypes in a controlled environment to evaluate their feasibility and effectiveness.

- Test failover and failback procedures to ensure the recovery process is reliable and can meet recovery time objectives (RTOs) and recovery point objectives (RPOs).

6. Implement:

- Develop a comprehensive plan for integrating IBM Cloud Virtual Servers into your disaster recovery strategy.

- Deploy the necessary virtual servers, storage, and network configurations in the IBM Cloud environment.

- Establish monitoring and alerting systems to keep track of server health and resource utilization.

7. Monitor and Iterate:

- Continuously monitor the performance of your disaster recovery solution using IBM Cloud Virtual Servers.

- Collect and analyse data on system performance, RTOs, RPOs, and overall effectiveness.

- Make necessary adjustments and improvements to optimize the disaster recovery process.

8. Communicate:

- Keep all relevant stakeholders informed about the progress and outcomes of your disaster recovery strategy with IBM Cloud Virtual Servers.

- Provide documentation and training to ensure that your IT team is well-prepared to execute the disaster recovery plan.

9. Document and Share Best Practices:

- Document the design, deployment, and performance of your disaster recovery solution using IBM Cloud Virtual Servers.

- Share best practices and lessons learned with the broader IT and disaster recovery community to promote knowledge sharing and improvement.

**Disaster recovery strategy:**

1. Backup and Restore:

- Regularly back up critical data, applications, and configurations.

- Implement automated backup solutions.

- Store backups both on-site and off-site to ensure redundancy.

- Test the restore process to ensure data recoverability.

2. High Availability (HA):

- Use redundant systems to eliminate single points of failure.

- Employ load balancing to distribute traffic across multiple servers.

- Implement failover mechanisms to automatically switch to a backup system in case of a failure.

3. Disaster Recovery as a Service (DRaaS):

- Consider outsourcing your disaster recovery to a specialized service provider.

- DRaaS providers offer cloud-based solutions for data backup, recovery, and failover.

4. Data Replication:

- Use data replication technologies to maintain real-time or near-real-time copies of data at a remote location.

- Replicate data to a secondary data center, cloud, or off-site facility.

5. Cloud-Based Disaster Recovery:

- Utilize cloud resources for disaster recovery, including backup storage, virtualization, and infrastructure.

- Cloud services offer scalability and flexibility, making them suitable for various disaster recovery needs.

6. Data Center Resilience:

- Build data Centre’s with resilience in mind, using redundant power supplies, cooling systems, and network connectivity.

- Consider geographical diversity to minimize the impact of regional disasters.

7. Failover and Failback Procedures:

- Develop documented procedures for failing over to backup systems and returning to normal operations (failback) once the primary system is restored.

8. Business Continuity Planning (BCP):

- Create a comprehensive business continuity plan that outlines how the organization will operate during and after a disaster.

- Include plans for communication, employee safety, and customer engagement.

9. Testing and Training:

- Regularly test disaster recovery plans and procedures to ensure they work as expected.

- Provide training to staff and stakeholders on their roles and responsibilities in a disaster recovery scenario.

10. Security Considerations:

- Implement security measures to protect data during the recovery process.

- Consider encryption, access controls, and secure communication for data in transit and at rest.

11. Documentation:

- Maintain up-to-date documentation of all disaster recovery procedures, contacts, and configurations.

**Backup Configuration:**

Backing up your configuration in disaster recovery is a critical aspect of ensuring that you can recover your systems and data in case of unexpected events such as hardware failures, natural disasters, cyberattacks, or other catastrophic incidents.

1. Identify Critical Configurations: Begin by identifying the critical configurations that are essential for your business operations. This may include server configurations, network settings, application configurations, security policies, and more.

2. Regular Backups: Implement a regular backup schedule for these configurations. The frequency of backups will depend on the rate of change and the importance of the configuration. Some configurations may require daily backups, while others can be done weekly or monthly.

3. Automate the Backup Process: Whenever possible, automate the backup process to ensure consistency and reduce the chance of human error. Use backup software or scripts to regularly capture and store the configuration data.

4. Version Control: Consider using version control systems (e.g., Git) for tracking changes to configuration files. This allows you to maintain a history of configurations and easily roll back to a previous version if necessary.

5. Off-Site Backups: Store backup copies of your configurations off-site or in a geographically separate location. This helps protect against disasters that could affect your primary data center or location.

6. Encryption: Ensure that the backup files are securely encrypted to protect sensitive configuration data. This is especially important for security-related configurations.

7. Testing: Regularly test your backup and restoration processes to make sure that they work as expected. This can help you identify and address any issues before a disaster occurs.

8. Documentation: Maintain clear documentation of the backup procedures and where the backup files are stored. This documentation should be accessible to relevant staff members involved in disaster recovery.

**Replication setup:**

Setting up a disaster recovery (DR) solution for IBM Cloud Virtual Servers involves ensuring that your data and workloads are protected and can be quickly restored in the event of a disaster or unexpected outage. IBM Cloud provides several tools and services that can help you implement a robust DR strategy. Here's a general outline of the steps you can take:

1. Assessment and Planning:

- Identify your critical workloads and data that need to be protected.

- Define your Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These metrics determine how often data is backed up and how quickly it needs to be restored.

2. Select a Disaster Recovery Solution:

- IBM Cloud offers various options for DR, including backup and recovery services like IBM Cloud Backup and IBM Cloud Object Storage, as well as hybrid cloud solutions like IBM Cloud Resiliency Orchestration.

- Choose the solution that best fits your needs based on your assessment and planning.

3. Replication Strategy:

- Set up data replication between your primary and secondary sites. IBM Cloud services, like IBM Cloud Object Storage, can be used to store and replicate data.

- You may consider synchronous replication for zero data loss or asynchronous replication for more flexibility in handling longer distances between your primary and secondary sites.

4. IBM Cloud Virtual Servers:

- Ensure that your IBM Cloud Virtual Servers are properly configured and set up in your primary and secondary data centres or regions.

- Make sure your virtual servers are regularly backed up, and the backups are replicated to your secondary location.

5. Network Configuration:

- Set up secure, high-speed connectivity between your primary and secondary sites. IBM Cloud offers VPN and Direct Link options for this purpose.

- Ensure that network configurations, including subnets and firewall rules, are consistent between the primary and secondary sites.

6. Testing and Validation:

- Regularly test your DR plan to ensure it works as expected. This includes performing failover and failback tests to your secondary site.

- Use automation and orchestration tools, if available, to streamline testing procedures.

7. Monitoring and Alerting:

- Implement monitoring tools to keep an eye on the health and performance of your virtual servers and replication processes.

- Set up alerting to notify you of any issues or anomalies in real-time.

8. Documentation:

- Maintain comprehensive documentation of your DR plan, including configurations, procedures, contact information, and any changes made over time.

9. Compliance and Security:

- Ensure that your DR solution complies with industry and regulatory standards, especially if you handle sensitive or regulated data.

- Implement strong security measures to protect your data during replication and in storage.

10. Regular Maintenance:

- Regularly review and update your DR plan to reflect changes in your infrastructure, applications, and business requirements.

- Test your plan periodically to validate its effectiveness.

11. Communication Plan:

- Ensure that all relevant stakeholders are aware of the DR plan, their roles and responsibilities, and the communication channels to be used during a disaster event.

**Recovery testing procedures:**

Recovery testing is a critical component of disaster recovery planning. It involves testing the effectiveness of your disaster recovery procedures to ensure that your systems and data can be successfully restored in the event of a disaster or system failure

1. Establish Testing Objectives:

- Clearly define the objectives and scope of the recovery testing. What systems, data, and processes will be tested, and what are the expected outcomes?

2. Document Your Recovery Plan:

- Ensure that you have a well-documented disaster recovery plan in place before conducting any tests. The plan should outline the steps to be taken during recovery.

3. Select the Right Test Environment:

- Set up a separate, isolated environment for testing to avoid impacting your production systems. This may involve using a dedicated test environment or a cloud-based environment.

4. Test Scenarios:

- Develop different recovery scenarios to mimic various disaster situations, such as hardware failures, data corruption, natural disasters, and cyber-attacks. Test both partial and complete system recoveries.

5. Prioritize Critical Systems:

- Prioritize the testing of critical systems and data to ensure that they can be recovered with minimal downtime.

6. Testing Frequency:

- Conduct recovery testing on a regular basis. The frequency of testing depends on the rate of change in your environment and your business requirements.

7. Full-Scale Testing:

- Periodically conduct full-scale recovery tests that simulate a complete disaster recovery. This ensures that all components of your recovery plan are thoroughly tested.

8. Partial Recovery Testing:

- Test partial recoveries to assess the ability to recover specific systems or data in isolation.

9. Data Validation:

- Verify the integrity of recovered data to ensure that it is consistent and accurate. This includes data stored in databases, file systems, and backups.

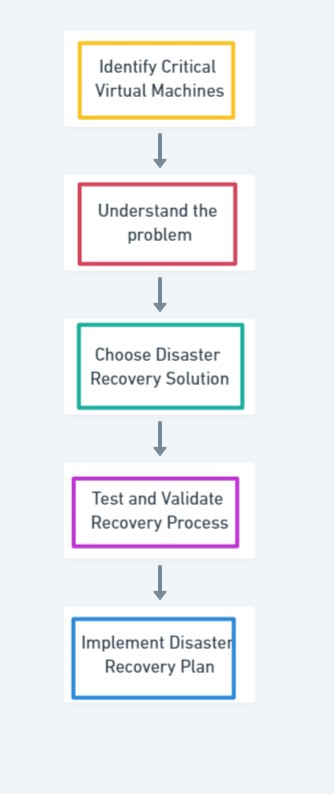
10. Infrastructure Testing:

- Test not only data recovery but also the recovery of infrastructure components, such as servers, network configurations, and virtual machines.

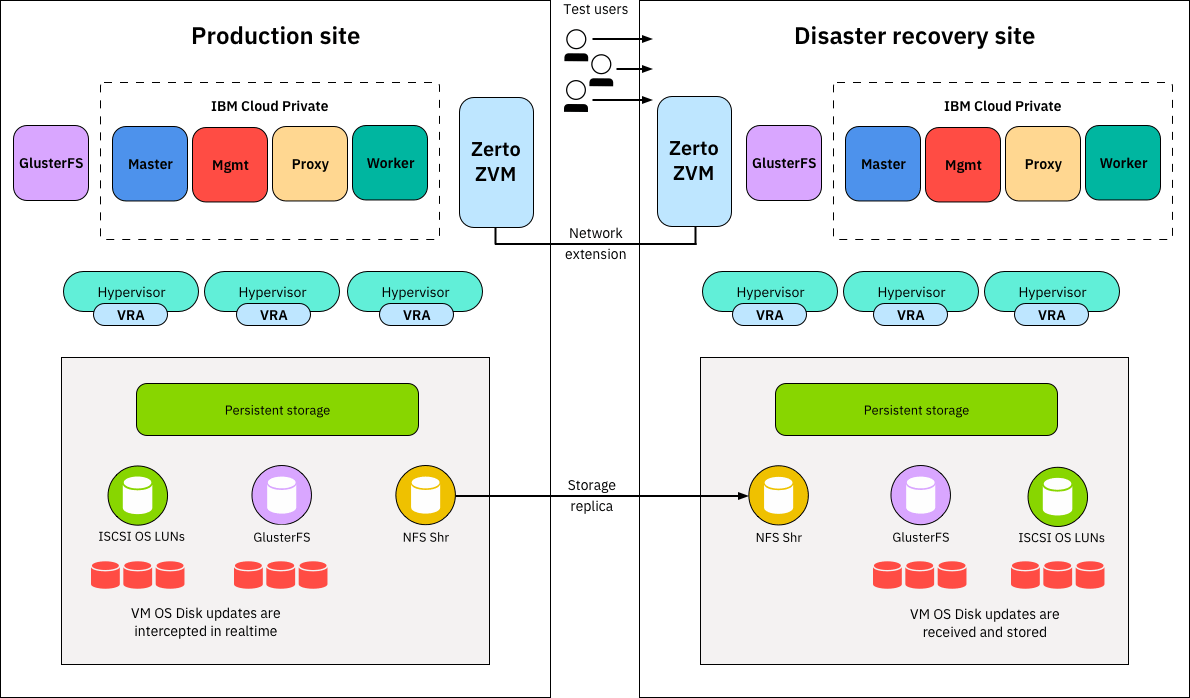
11. Application Testing:

- Test the recovery of applications, including the reinstallation, reconfiguration, and testing of software and services.

**Flow chart:**



**Technology architecture:**



Designing a disaster recovery (DR) architecture using IBM Cloud Virtual Servers involves creating a resilient, redundant, and geographically distributed infrastructure to ensure the availability of critical applications and data in the event of a disaster. Here's detailed technology architecture for disaster recovery with IBM Cloud Virtual Servers:

1. Assessment and Planning:

- Identify your critical workloads, applications, and data that need disaster recovery protection.

- Define your Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to determine how quickly you need to recover and how much data loss is acceptable.

2. Primary Data Center:

- Your primary data center hosts your production workloads and applications. It includes IBM Cloud Virtual Servers and related resources.

3. Secondary Data Center:

- Establish a secondary data center in a geographically separate location to provide redundancy. This secondary site is used for disaster recovery.

- Deploy IBM Cloud Virtual Servers with identical configurations to the primary data center.

- Ensure the secondary data center is equipped with the necessary network, power, and cooling infrastructure.

4. Data Replication:

- Implement data replication mechanisms to keep data synchronized between the primary and secondary data centres. IBM Cloud offers several options:

- IBM Cloud Object Storage: Use it for backup and replication of data.

- Database Replication: For databases, consider IBM Db2, PostgreSQL, or other databases with built-in replication features.

- Third-Party Replication Solutions: Use third-party solutions like IBM Spectrum Virtualize for block-level replication or file synchronization tools for file-based replication.

5. Network Connectivity:

- Ensure redundant and high-speed network connectivity between your primary and secondary sites. IBM Cloud offers Direct Link and VPN services to establish secure and reliable connections.

6. Load Balancing:

- Use load balancers to distribute traffic between the primary and secondary sites. This enables seamless failover and ensures high availability.

7. Failover Mechanism:

- Implement an automated failover mechanism to switch traffic from the primary to the secondary data center in the event of a disaster. This can be achieved through tools like IBM Cloud's Load Balancers and automation scripts.

- Set up DNS failover to direct traffic to the secondary data center when the primary is unavailable.

8. Automation and Orchestration:

- Utilize automation and orchestration tools such as Ansible, Terraform, or IBM Cloud Automation Manager to automate the failover and failback processes. These tools can streamline the recovery procedures and minimize human error.

9. Monitoring and Alerts:

- Set up monitoring tools to continuously track the health and performance of your systems.

- Configure alerting systems to notify relevant personnel when anomalies or failures occur.

10. Testing:

- Regularly test your disaster recovery plan through planned failover drills and exercises to ensure it works as expected.

11. Documentation:

- Maintain comprehensive documentation of your disaster recovery plan, including procedures, contact information, configurations, and testing results.

12. Security:

- Implement robust security measures in both the primary and secondary environments, including encryption, access control, and firewall rules.

13. Compliance:

- Ensure your disaster recovery plan complies with relevant regulatory requirements and industry standards.

14. Vendor Support:

- Engage with IBM's support and services to ensure you have access to the necessary expertise and resources for managing your DR solution effectively.

This technology architecture is designed to provide a high level of resilience and availability for your critical workloads hosted on IBM Cloud Virtual Servers while minimizing the impact of disasters or outages. Remember to customize this architecture to meet your organization's specific requirements and constraints.

**Modules description:**

To implement a disaster recovery solution with IBM Cloud Virtual Servers, you can break down the architecture into different modules or components. Each module serves a specific purpose in ensuring the availability and recovery of your systems in case of a disaster. Here's a detailed description of each module:

1. Primary Data Center:

- This is your primary environment where your production workloads and applications are hosted.

- It includes IBM Cloud Virtual Servers, storage, networking, and related resources required for normal operations.

2. Secondary Data Center:

- The secondary data center is the disaster recovery site, located in a geographically separate location for redundancy.

- This module consists of IBM Cloud Virtual Servers with configurations similar to those in the primary data center.

- Ensure it has its own network, power, and cooling infrastructure.

3. Data Replication:

- Data replication mechanisms are critical for keeping data synchronized between the primary and secondary data centres.

- Choose the appropriate data replication methods based on the type of data and applications you're using. This may include IBM Cloud Object Storage for file backups or database-specific replication solutions.

4. Failover Mechanism:

- This module encompasses the automated failover mechanisms that enable the smooth transition of traffic from the primary to the secondary data center when a disaster occurs.

- IBM Cloud Load Balancers and automation scripts are typically used for this purpose.

5. Monitoring and Alerts:

- Implement monitoring tools that continuously monitor the health and performance of systems in both the primary and secondary data canters.

- Configure alerting systems to notify relevant personnel when anomalies or failures are detected.

6. Testing and Validation:

- Regularly test your disaster recovery plan to ensure that it works as expected. This module includes planned failover drills and exercises to validate the recovery procedures.

- Document the results of these tests for reference and improvement.

7. Documentation and Procedures:

- Maintain detailed documentation of your disaster recovery plan, including step-by-step procedures, contact information, and configuration details.

- This module serves as the foundation for effective disaster recovery operations.

8. Security:

- Implement robust security measures in both the primary and secondary environments, including encryption, access control, and firewall rules.

- Security is essential to protect your data and applications during disaster recovery.

**Algorithm and Technology used:**

1. Data Replication Technologies:

- Synchronous Replication: Data is replicated in real-time between the primary and secondary data centers. This ensures that both sites have identical data at all times.

- Asynchronous Replication: Data is periodically copied from the primary to the secondary site, which may introduce a slight delay but is suitable for long-distance disaster recovery to minimize latency.

2. Storage Area Network (SAN):

- SAN technology provides high-speed, reliable data storage and access, often used in DR setups to ensure data can be quickly accessed and recovered.

3. Data Deduplication and Compression:

- These technologies reduce the amount of data transferred between the primary and secondary sites, making replication more efficient.

4. Network Technologies:

- Direct Link and VPN: IBM Cloud offers these technologies to establish secure and reliable network connections between the primary and secondary data centers.

- Content Delivery Networks (CDNs): CDNs can be used to deliver content and applications more efficiently, reducing latency in disaster recovery scenarios.

5. Load Balancing Algorithms:

- When failing over to a secondary site, load balancers use various algorithms to distribute traffic effectively. Common algorithms include round-robin, least connections, and IP hash.

6. Automated Failover and Failback Algorithms:

- Automated scripts and orchestration tools use predefined algorithms to detect primary site failures and initiate the failover process. These algorithms are designed to minimize downtime and data loss.

7. Data Backup Algorithms:

- Backup algorithms define backup frequency, retention periods, and data management. They ensure data consistency and meet recovery point objectives (RPO).

8. Replication Conflict Resolution Algorithms:

- In the case of asynchronous replication, conflict resolution algorithms handle situations where data modifications occur simultaneously on both the primary and secondary sites. These algorithms determine which changes should take precedence.

9. Security Algorithms:

- Encryption algorithms are crucial for securing data in transit and at rest. They ensure data integrity and confidentiality during the disaster recovery process.

10. Monitoring and Alerting Algorithms:

- Monitoring systems use various algorithms to detect anomalies and deviations from expected system behaviour. Alerting algorithms then trigger notifications to administrators or automated systems of potential issues.

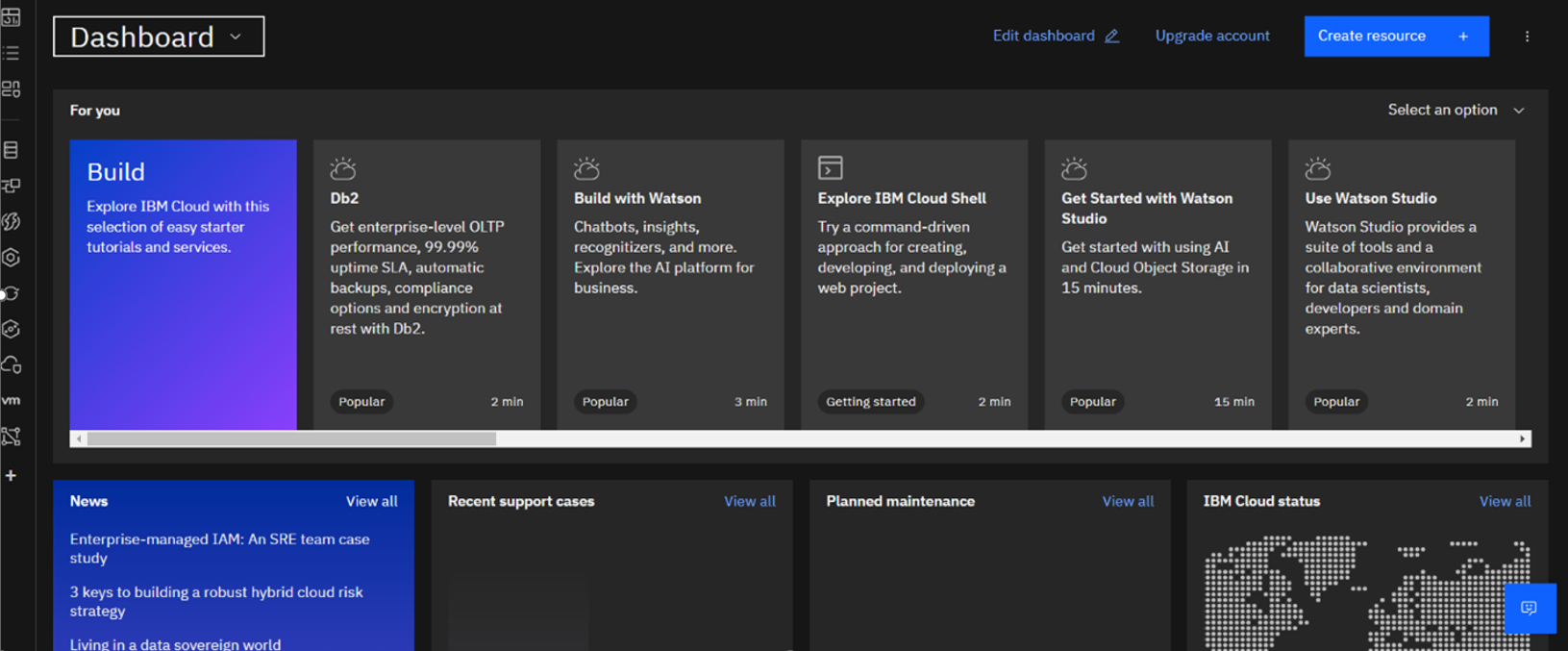
11. Failback Algorithms:

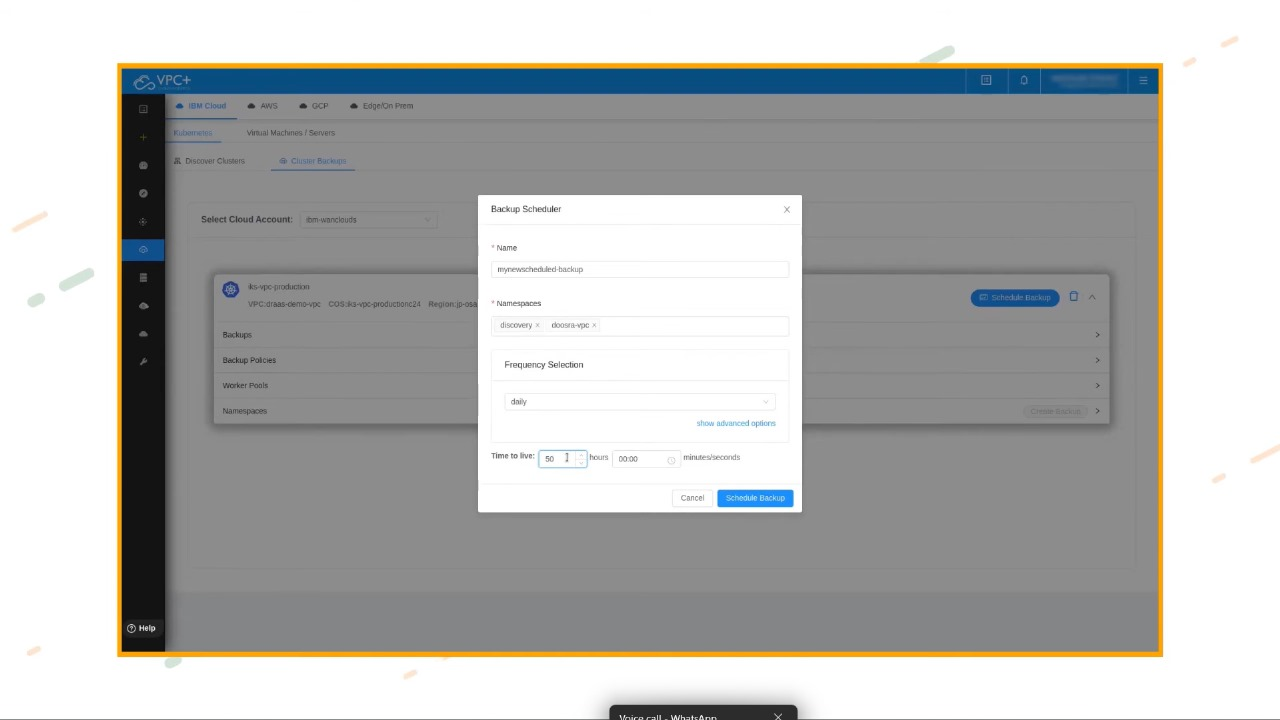
- When transitioning back to the primary data center after a disaster, failback algorithms ensure a smooth and controlled return to normal operations.

**Project development steps and screenshot:**

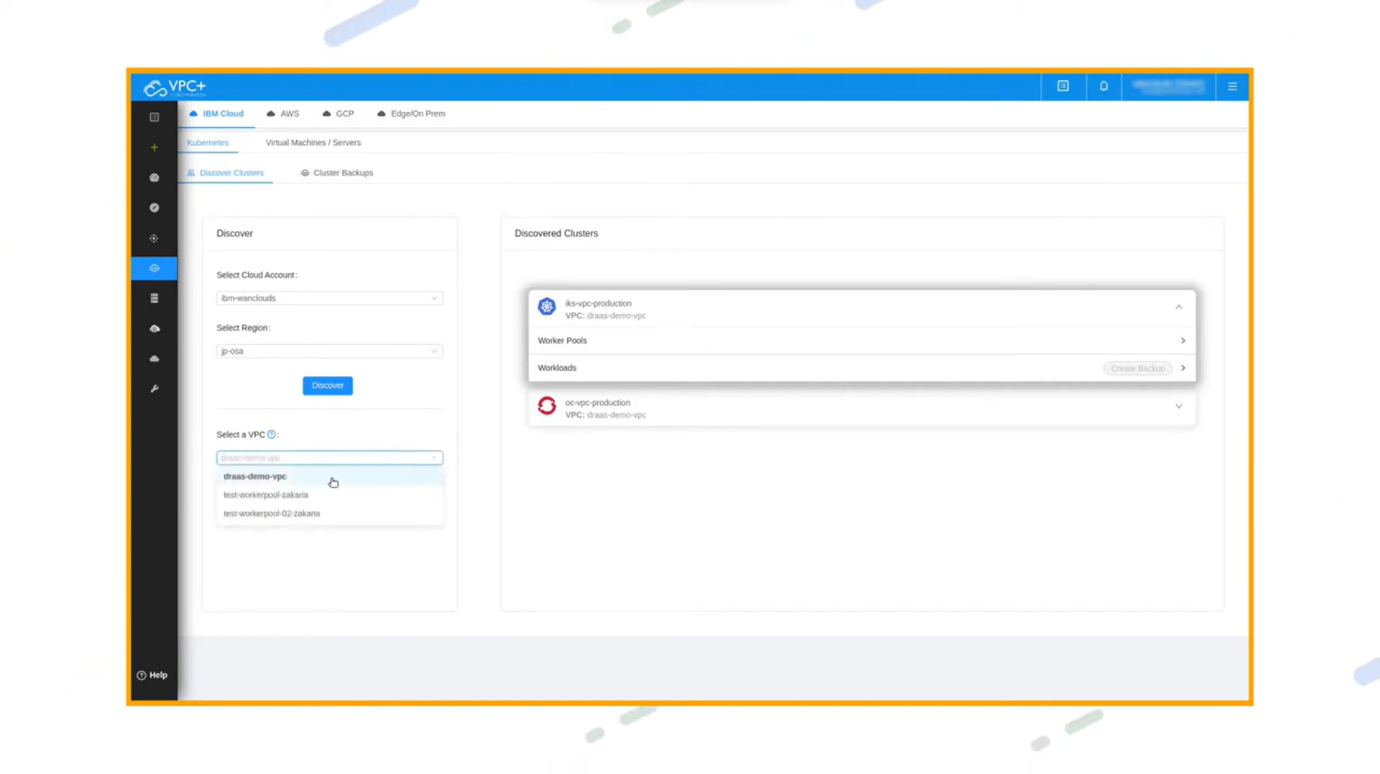
**Platform implemented: IBM Cloud**

**Create the ibm account .**

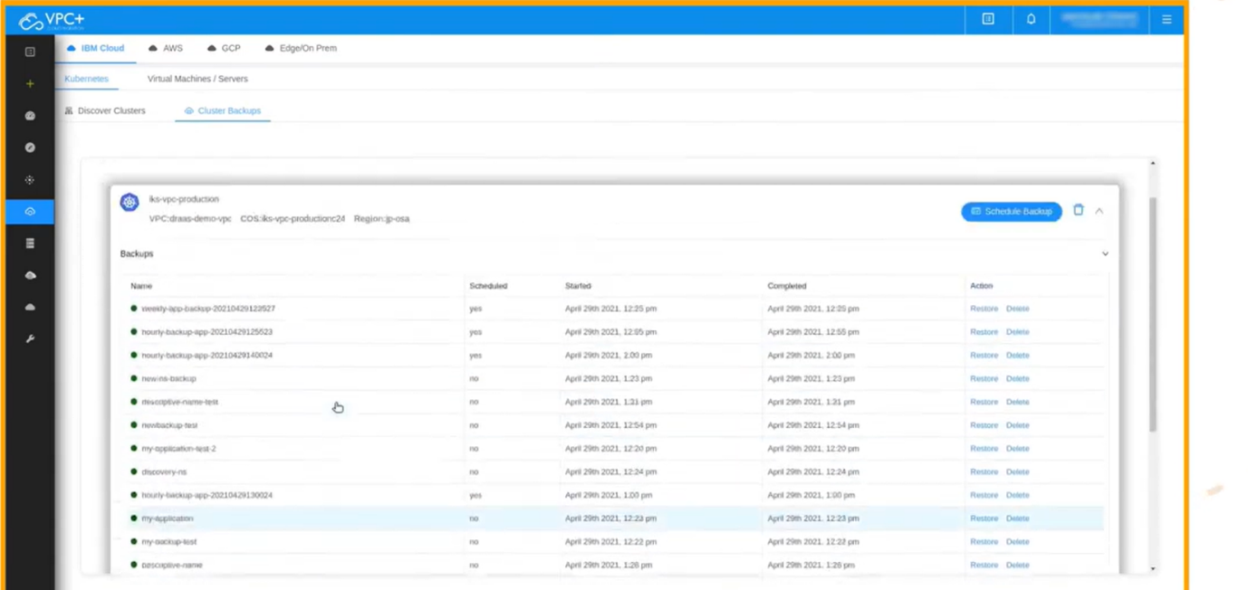




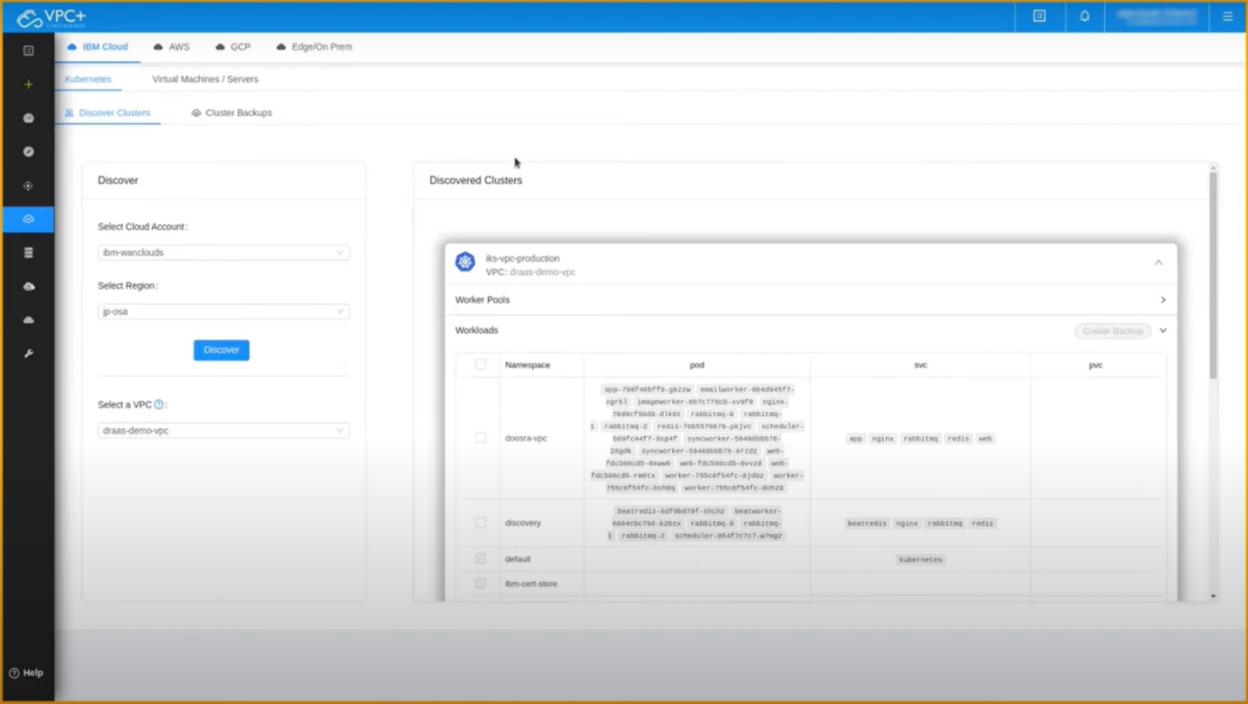
**Choose the files to restore.**

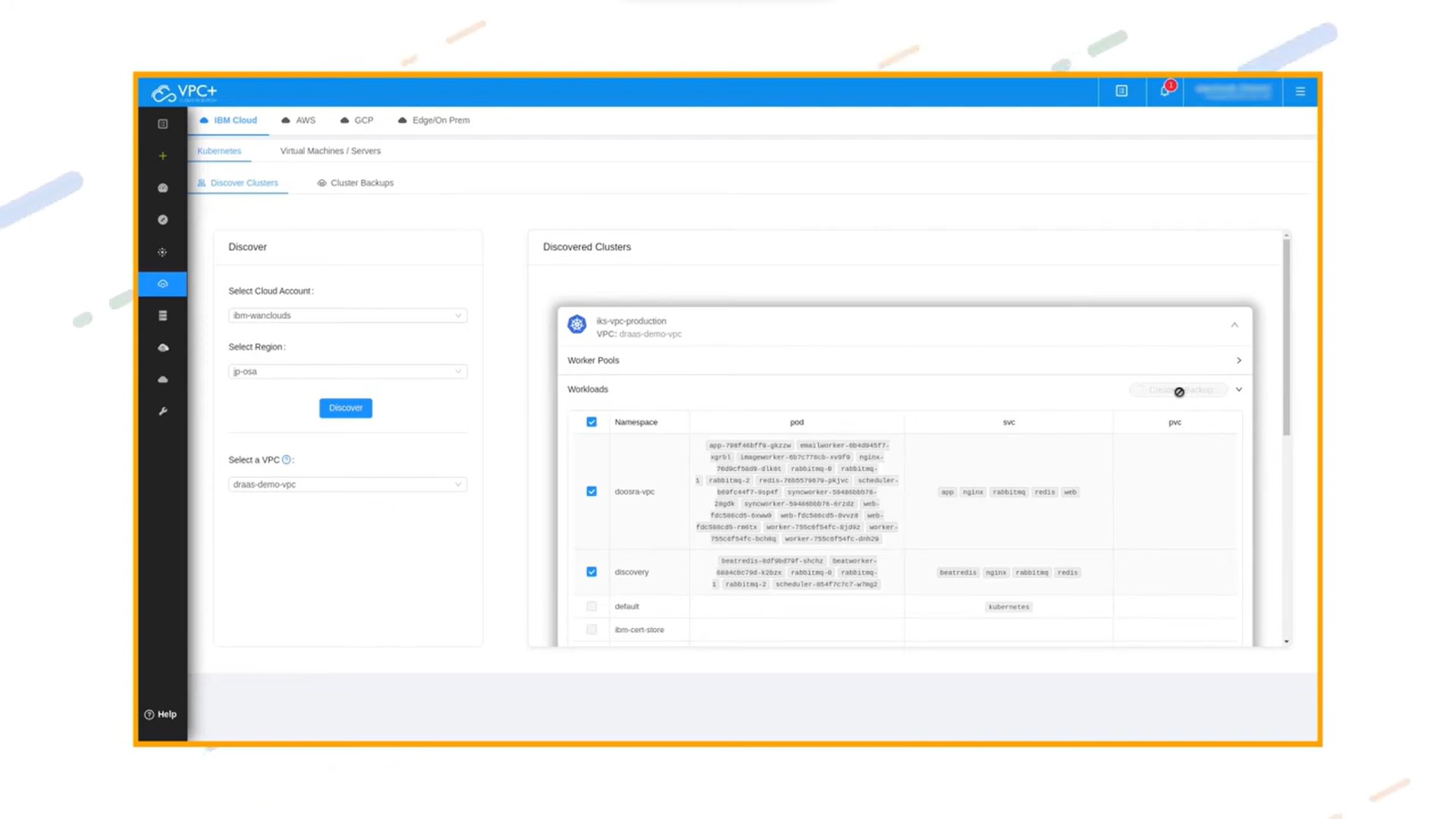


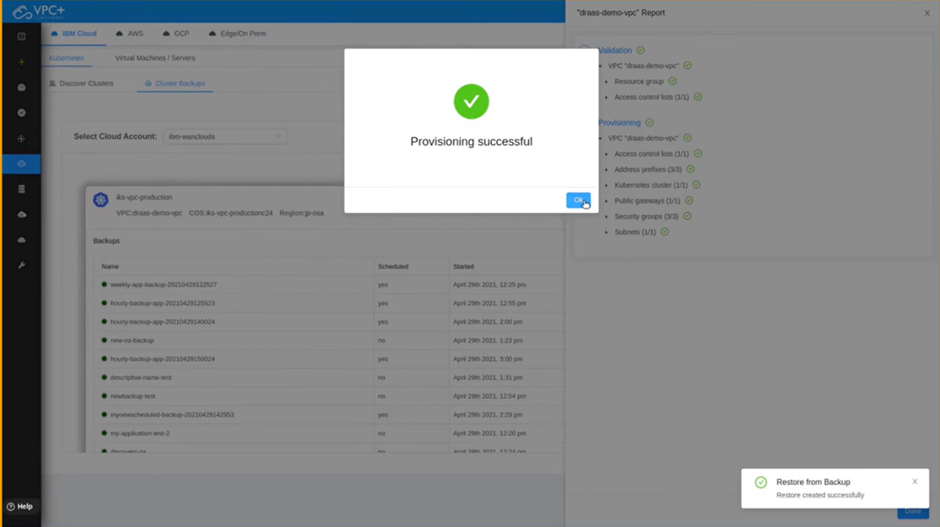
**After the backup the go cat log.**

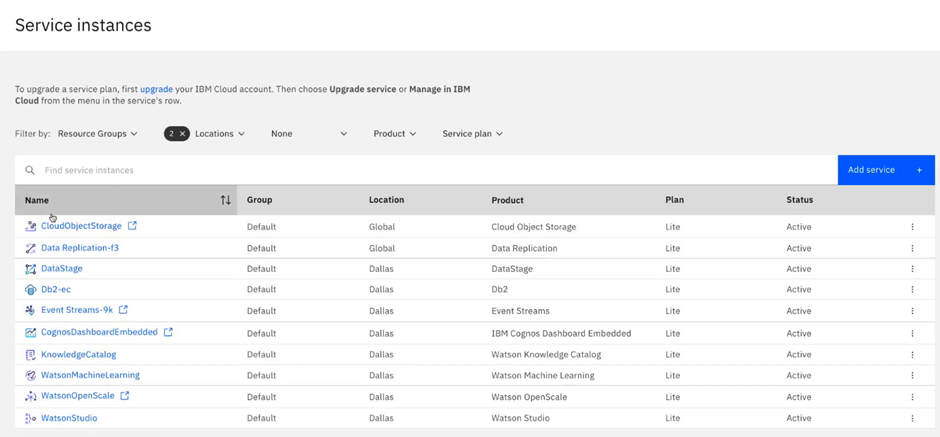


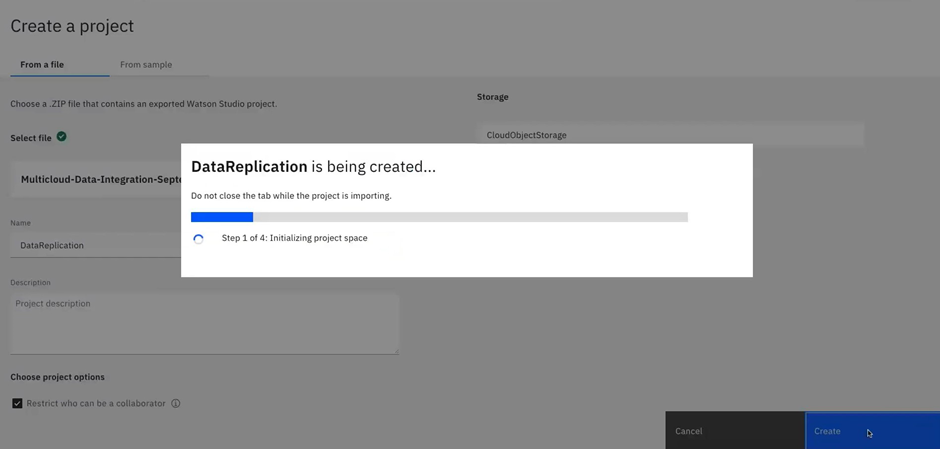
**Backup the files.**





 Cloud backup is successfully stored.

Go to service instance.



Data replication is done.

**Conclusion:**

we successfully created a disaster recovery plan using IBM Cloud Virtual Servers. By following the problem definition, design thinking, development, and documentation phases, we developed a plan that safeguards business operations and ensures continuity for an on-premises virtual machine in unforeseen events. The plan includes backup configuration, replication setup, recovery testing, and aligns with the organization's overall business continuity strategy. As the guardian of business continuity, we secure the future of the organization and provide peace of mind in the face of disasters.