Disaster Recovery with IBM Cloud Virtual Servers

Phase 1: Problem Definition and Design Thinking

Problem Definition:

The project involves creating a disaster recovery plan using IBM Cloud Virtual Servers. The objective is to safeguard business operations by developing a plan that ensures continuity for an on-premises virtual machine in unforeseen events. This plan will include setting up backup strategies, configuring replication, testing the recovery process, and guaranteeing minimal downtime. The project encompasses defining the disaster recovery strategy, implementing backup and replication, validating recovery procedures, and ensuring business continuity.

Design Thinking:

1. Disaster Recovery Strategy: Define the disaster recovery strategy and objectives, including recovery time objectives (RTO) and recovery point objectives (RPO).
2. Backup Configuration: Configure regular backups of the on-premises virtual machine to capture critical data and configurations.
3. Replication Setup: Implement replication of data and virtual machine images to IBM Cloud Virtual Servers to ensure up-to-date copies.
4. Recovery Testing: Design and conduct recovery tests to validate the recovery process and guarantee minimal downtime.
5. Business Continuity: Ensure that the disaster recovery plan aligns with the organization's overall business continuity strategy.

ENSURING BUSINESS CONTINUITY: DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

INTRODUCTION

Ensuring Business Continuity

Disaster recovery is crucial for businesses to minimize downtime and ensure uninterrupted operations. With **IBM Cloud Virtual Servers**, organizations can leverage scalable and secure infrastructure to protect their critical data and applications. This presentation will explore the key features and benefits of IBM Cloud Virtual Servers for disaster recovery.

DISASTER RECOVERY CHALLENGES

Addressing Key Challenges
Disaster recovery poses several challenges, including data loss, system downtime, and infrastructure costs. **IBM Cloud Virtual Servers** offer a comprehensive solution by providing automated backups, seamless failover, and cost-effective scalability. By leveraging the power of the cloud, businesses can ensure business continuity and minimize the impact of unforeseen events.

BENEFITS OF IBM CLOUD VIRTUAL SERVERS

Key Benefits

Flexibility: Easily scale resources up or down based on demand.
Reliability: High availability and redundancy for critical workloads.
Security: Robust data protection and encryption mechanisms.
Cost Efficiency: Pay only for the resources used, reducing infrastructure costs.
With IBM Cloud Virtual Servers, businesses can achieve efficient disaster recovery while optimizing their IT budget.

DISASTER RECOVERY PROCESS

Ensuring Continuity

Backup: Regularly back up critical data and applications.

Replication: Replicate data to a secondary site for redundancy.

Failover: Automatically switch to the secondary site in case of a disaster.

Recovery: Restore operations and data to ensure business continuity.

IBM Cloud Virtual Servers streamline the disaster recovery process, enabling organizations to quickly recover from disruptions.

IBM Cloud Virtual Servers Features

Key Features

Virtualization: Run multiple virtual servers on a single physical server.

Scalability: Easily add or remove resources as needed.

Security: Built-in security measures to protect against threats.

Monitoring: Real-time monitoring and alerts for proactive management.

IBM Cloud Virtual Servers provide a robust infrastructure for disaster recovery, ensuring efficient and secure operations.

CONCLUSION

Ensuring Business Continuity

With the increasing importance of disaster recovery, organizations need a reliable and scalable solution. **IBM Cloud Virtual Servers** offer the perfect combination of flexibility, reliability, security, and cost efficiency. By leveraging the power of the cloud, businesses can ensure uninterrupted operations and minimize the impact of potential disasters. Embrace IBM Cloud Virtual Servers for a robust disaster recovery strategy.

Thanks!

DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

Project Title: Disaster Recovery With IBM Cloud Virtual Servers.

Problem Statement :-

- The problem statement emphasizes the importance of effective disaster recovery planning for organizations using IBM Cloud virtual servers. It identifies six key challenges in this context:

1. **Ensuring Data Resilience:** Protecting critical data and applications on IBM Cloud servers during disasters.
2. **Minimizing Downtime:** Reducing service disruption and financial losses by swift recovery of virtual servers.
3. **Cost Efficiency:** Balancing the cost of disaster recovery with the benefits of business continuity.
4. **Compliance and Security:** Meeting data protection and security requirements while maintaining compliance.

5. **Automation and Testing:** Implementing automated disaster recovery procedures and regular testing.

6. **Scalability and Flexibility:** Adapting the disaster recovery plan to changing business needs.

Addressing these challenges requires careful planning, deep knowledge of IBM Cloud services, and a tailored disaster recovery strategy to ensure business continuity and data integrity in the face of unexpected disasters.

Method of Approach with Implementation :-

Creating a complete IBM Watson-based solution for the problem statement outlined would require multiple services, including Natural Language Understanding (NLU) for text analysis, Watson Assistant for chatbot interactions, and potentially other IBM Cloud services for managing the disaster recovery plan. Here's a simplified example of how you might integrate Watson services into a chatbot for discussing disaster recovery:

PROGRAME:

```
from ibm_watson import AssistantV2

from ibm_cloud_sdk_core.authenticators import IAMAuthenticator


# Set up your IAM credentials
```

```
authenticator = IAMAuthenticator('YOUR_API_KEY')

# Create an instance of the Assistant service
assistant = AssistantV2(
    version='2021-06-14',
    authenticator=authenticator
)

# Set the URL for your Watson Assistant instance
assistant.set_service_url('YOUR_SERVICE_URL')

# Create a session
response = assistant.create_session(
    assistant_id='YOUR_ASSISTANT_ID'
)
session_id = response.get_result()['session_id']

# User input for the chatbot
user_input = "What are the key challenges in disaster recovery with IBM Cloud virtual servers?"

# Send user input to the assistant
```

```
response = assistant.message(
    assistant_id='YOUR_ASSISTANT_ID',
    session_id=session_id,
    input={
        'message_type': 'text',
        'text': user_input
    }
)

# Get the response from the chatbot
bot_response = response.get_result()
print(bot_response['output']['generic'][0]['text'])

# Close the session
assistant.delete_session(
    assistant_id='YOUR_ASSISTANT_ID',
    session_id=session_id
)
```

Addressing these challenges requires careful planning, deep knowledge of IBM Cloud services, and a tailored disaster recovery strategy to ensure business continuity and data integrity in the face of unexpected disasters.

DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

TEAM MEMBERS:

SALAI OLIR MUTHU.S
SWATHI.V
ANUPRIYA.A
SHALINI.R
PRAVEENA.M

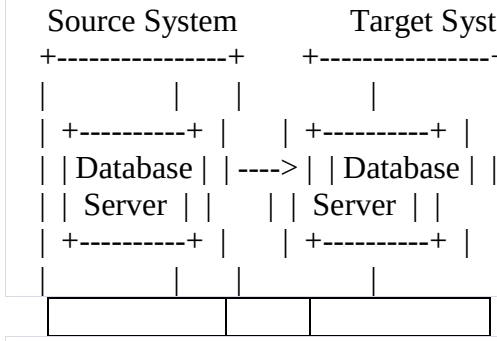
PROJECT TITLE:DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

INTRODUCTION:

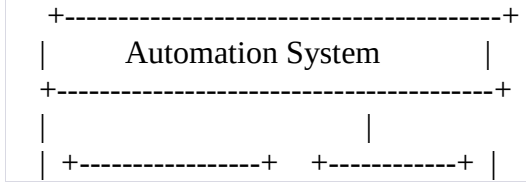
Disaster recovery is a critical aspect of any organization's IT infrastructure strategy, ensuring the continuity of business operations in the face of unexpected disruptions. IBM Cloud Virtual Servers offer a powerful solution to help businesses plan for and mitigate the impact of disasters on their digital assets. In this introduction, we will explore the key concepts and benefits of disaster recovery with IBM Cloud Virtual Servers.

IBM Cloud Virtual Servers provide a flexible and scalable computing environment in the cloud, making it an ideal choice for designing a robust disaster recovery plan. In the event of unforeseen disasters, such as natural calamities, cyberattacks, or system failures, having a reliable disaster recovery strategy becomes paramount to maintain business continuity.

1. **Resilience:** IBM Cloud's global network of data centers ensures high availability and redundancy. By leveraging virtual servers across multiple geographical regions, businesses can maintain their critical workloads even if one region is impacted by a disaster.
2. **Data Replication:** Disaster recovery often involves replicating critical data to a secondary location. IBM Cloud provides data replication and backup services to ensure that your data is safe and accessible, no matter what happens to your primary environment.



3. **Automation:** Automating the failover and failback processes is crucial for minimizing downtime. IBM Cloud offers automation tools and APIs to streamline disaster recovery operations, reducing human error and response times.



```
| |  Sensors      |   | Actuators  | |
| | (e.g., Temp,  |   | (e.g., Motors,| |
| |  Pressure, etc.)|  |  Valves, etc.)| |
| +----------------+   +------------+ |
|          |          |         |
| +----------------+   +------------+ |
| |  Control Logic |   |  PLC (Programmable| |
| |  (e.g., PLC)  |   |  Logic Controller) | |
| +----------------+   +------------+ |
|          |          |         |
| +----------------+   +------------+ |
| |  HMI (Human   |   |  Communication | |
| | Machine Interface)| |  Network  | |
| +----------------+   +------------+ |
|                           |
```

4. **Customization:** IBM Cloud Virtual Servers can be tailored to meet specific business needs. Whether you need a warm standby environment, a hot site for immediate failover, or a hybrid solution, you can configure your disaster recovery setup to match your exact requirements.
5. **Cost Efficiency:** IBM Cloud's pay-as-you-go model means you only pay for the resources you use. This cost efficiency makes disaster recovery with virtual servers a cost-effective solution for businesses of all sizes.
6. **Testing and Monitoring:** Regular testing and monitoring of your disaster recovery plan are crucial to ensure it functions as expected. IBM Cloud provides tools and resources for testing and validating your disaster recovery processes.

By harnessing the power of IBM Cloud Virtual Servers for disaster recovery, organizations can significantly enhance their resilience, minimize downtime, and protect critical data and applications. This introduction sets the stage for a deeper dive into the strategic planning and implementation of a robust disaster recovery solution with IBM Cloud Virtual Servers, helping businesses maintain operational continuity in the face of adversity.

Code snippet:

1.Automated Backup Script (AWS S3):

This script schedules automated backups of data to Amazon S3. You can use AWS Lambda to schedule this script.

pythonCopy code

```
import boto3
```

```
import datetime

s3 = boto3.client('s3')
source_bucket = 'your-source-bucket'
backup_bucket = 'your-backup-bucket'

def lambda_handler(event, context):
    timestamp = datetime.datetime.now().strftime("%Y-%m-%d-%H-%M-%S")
    backup_object_key = f'backup/{timestamp}/your-data-file.zip'

    s3.copy_object(Bucket=backup_bucket, CopySource=f'/{source_bucket}/your-data-file.zip', Key=backup_object_key)
```

2.Database Backup and Restore (PostgreSQL):

This script automates the backup and restore of a PostgreSQL database. You can schedule it with a cron job.

```
# Backup
pg_dump -U youruser -h yourdbhost -d yourdatabase -f /path/to/backup.sql

# Restore
psql -U youruser -h yourdbhost -d yourdatabase -f /path/to/backup.sql
```

3.Automated Snapshot (Azure Virtual Machines):

This script takes a snapshot of an Azure virtual machine to create a point-in-time backup.

```
# Create a snapshot
az vm create --resource-group your-resource-group --name your-vm-name --image your-snapshot-name --no-wait
```

4.Script for Monitoring and Alerting:

You can use a script to continuously monitor the health of your services and infrastructure, and trigger alerts in case of issues. This example uses Python and the AWS SDK for monitoring AWS CloudWatch alarms

```
import boto3

def check_cloudwatch_alarms():
    cloudwatch = boto3.client('cloudwatch')
    alarms = cloudwatch.describe_alarms()
```

```
    for alarm in alarms['MetricAlarms']:
        if alarm['StateValue'] == 'ALARM':
            # Trigger alert action (e.g., send notification)
            # Implement your alerting logic here
            print(f"Alarm '{alarm['AlarmName']}' is in ALARM state.")

# Set up a scheduled job (e.g., using cron) to run this script periodically
```

Conclusion:

Disaster recovery is a critical aspect of business and IT operations. It ensures the continuity of business activities in the event of unforeseen disruptions, be they natural disasters, cyberattacks, or system failures. Key points to remember include the diversity of approaches, the importance of automation and testing, the benefits of cloud-based solutions, and the significance of data security and compliance. Effective planning, preparedness, communication, and team coordination are vital, and disaster recovery is an ongoing, adaptable process. In our interconnected world, disaster recovery is not just about physical threats but also cyber risks, making it essential for organizational resilience and sustainability.

Cloud Application Development

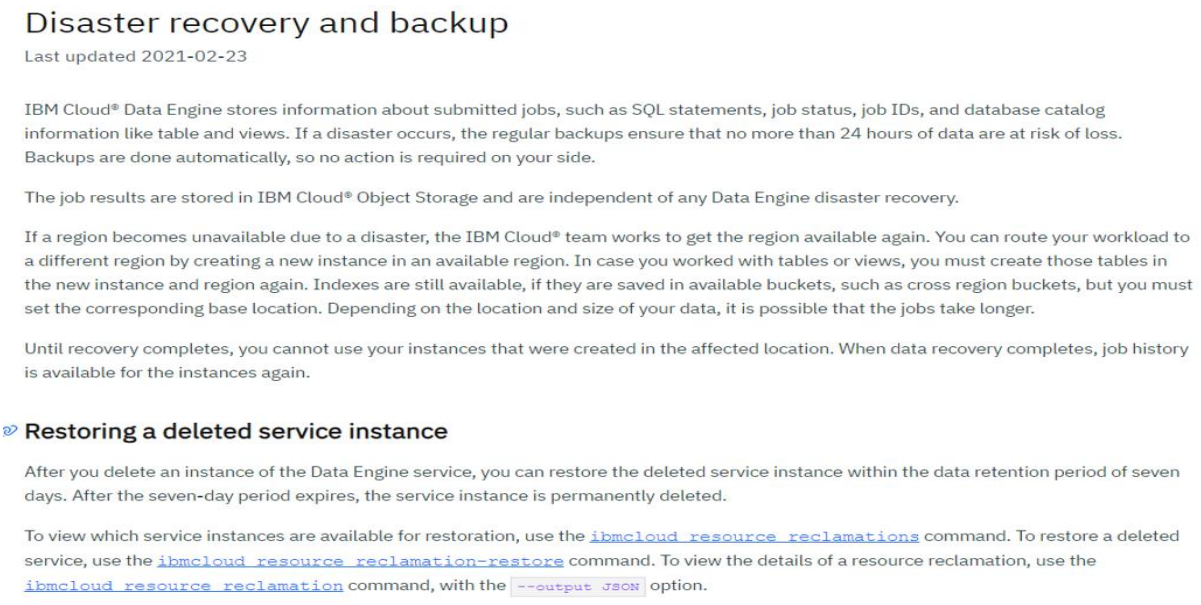
Disaster Recovery with IBM Cloud Virtual Servers

Phase 4

- Continue building the disaster recovery plan by configuring replication and testing recovery procedures.
- Implement replication of data and virtual machine images from on-premises to IBM Cloud Virtual Servers.
- Conduct recovery tests to ensure that the disaster recovery plan works as intended. Simulate a disaster scenario and practice recovery procedures.

Continue:

Here we can do the testing, recovery and backup step using VPC and VM are done



Disaster recovery and backup

Last updated 2021-02-23

IBM Cloud® Data Engine stores information about submitted jobs, such as SQL statements, job status, job IDs, and database catalog information like table and views. If a disaster occurs, the regular backups ensure that no more than 24 hours of data are at risk of loss. Backups are done automatically, so no action is required on your side.

The job results are stored in IBM Cloud® Object Storage and are independent of any Data Engine disaster recovery.

If a region becomes unavailable due to a disaster, the IBM Cloud® team works to get the region available again. You can route your workload to a different region by creating a new instance in an available region. In case you worked with tables or views, you must create those tables in the new instance and region again. Indexes are still available, if they are saved in available buckets, such as cross region buckets, but you must set the corresponding base location. Depending on the location and size of your data, it is possible that the jobs take longer.

Until recovery completes, you cannot use your instances that were created in the affected location. When data recovery completes, job history is available for the instances again.

Restoring a deleted service instance

After you delete an instance of the Data Engine service, you can restore the deleted service instance within the data retention period of seven days. After the seven-day period expires, the service instance is permanently deleted.

To view which service instances are available for restoration, use the ibmcloud resource reclamations command. To restore a deleted service, use the ibmcloud resource reclamation-restore command. To view the details of a resource reclamation, use the ibmcloud resource reclamation command, with the --output JSON option.

This is the whole process to do the backup and recovery of the data using IBM cloud virtual servers

Migration Overview

Your cloud migration process will consist of the following steps:

Creating your account on VPC+

To use VPC+ by Wanclouds, you will first need to sign up for an account. You can learn how to do that here.

Adding your Cloud account to VPC+

In order for VPC+ to access details of your existing environment, you must add your Cloud account information. Read the full guide here.

Discovering your existing environment

After you sign up for a VPC+ account and add your Cloud accounts, the VPC+ tool can discover your current infrastructure resources that can be migrated. More details can be found here.

Editing your discovered resources

VPC+ creates a workspace based on your existing environment where you can add, delete, and edit any section of your environment before migrating. Learn how to edit your workspace here.

Provisioning your resources in the new environment

VPC+ lets you either provision your entire environment or select the components that you want to provision, allowing you to migrate the rest at a later time. Read more on provisioning here.

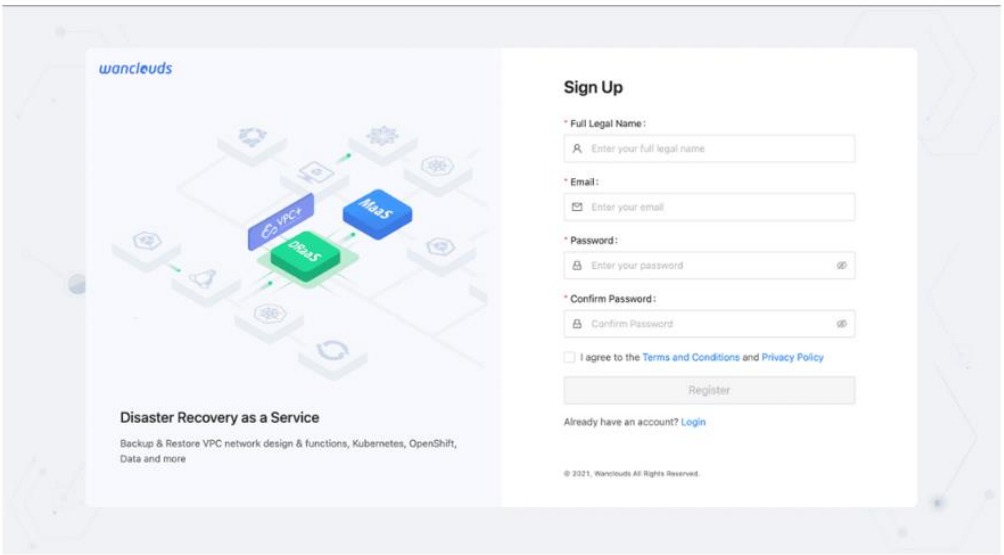
These are the main steps to do the recovery and backup process

The below steps to create an account on VPC

Creating your account

To create your account on VPC+, follow these instructions

1. Visit https://vpc.wanclouds.net and Register an account.



Adding your cloud accounts

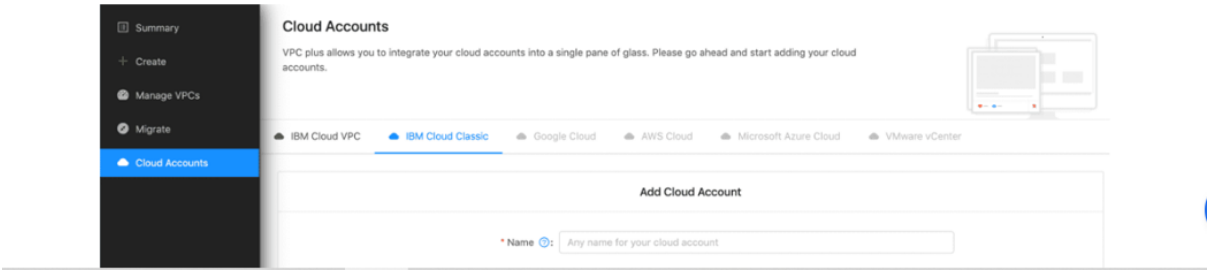
You must add a cloud account for VPC+ to be able to discover your existing environment. Adding a cloud account on VPC+ will let you:

- Discover your existing environment
- Migrate it to your desired cloud
- Manage it with the ability to add, delete or edit sections of your VPC

To add a cloud account, follow the instructions for each Cloud provider below:

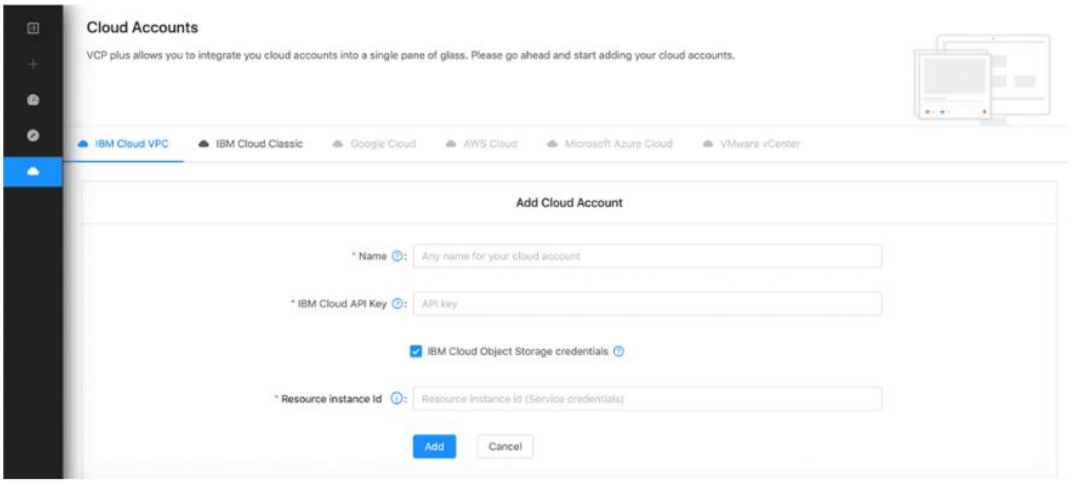
IBM Cloud

1. Navigate to the sidebar and click on **Cloud Accounts**.
2. Under the **IBM Cloud Classic** tab, click on **Add Account** to add your **Cloud account**.



Here click on add cloud account then we get the below page

3. Give this account a **Name** and enter the **Username** and **API Key** of your **IBM Cloud** classic infrastructure. This will be used to discover your current environment.
4. Under the tab, **IBM Cloud VPC**, add your **VPC** infrastructure **API Key** and your **IBM Cloud Object Storage (COS)** Resource Instance ID. Your **API** key will be used to migrate from **Classic Infrastructure** to **VPC Infrastructure** and your **IBM Cloud Object Storage (COS)** Resource Instance ID will be used to migrate primary or secondary volumes of your **Virtual Server Instances (VSIs)**.



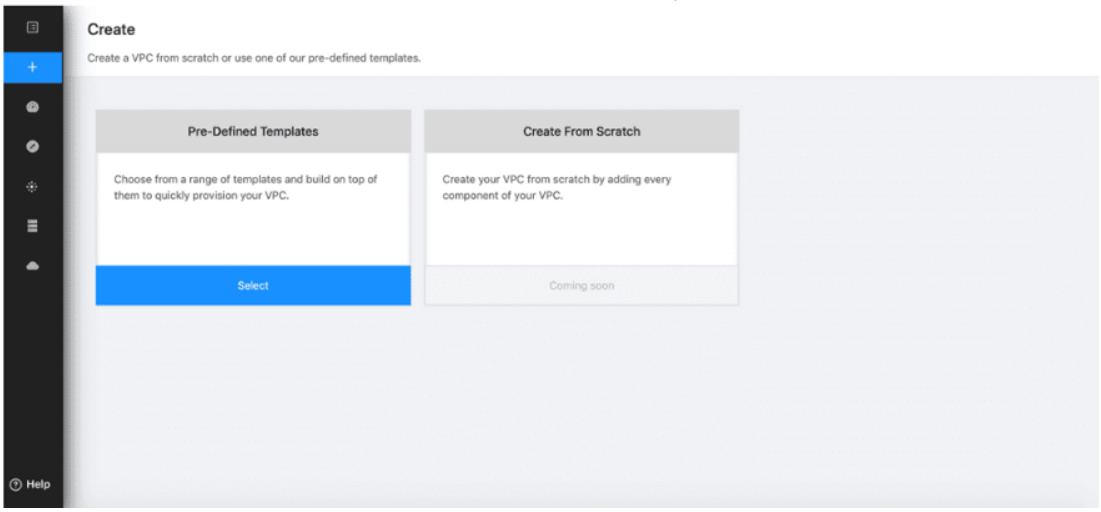
Here we give the API key and name then click on add the account will be added

Using Templates to Create Your VPC

Pre-defined templates are a great way to kick-start your VPC journey without getting into each minute detail. We have curated these templates keeping in mind the most common use cases of virtual private clouds. When you create a VPC using a template, a basic structure is provisioned and you can build on top of that.

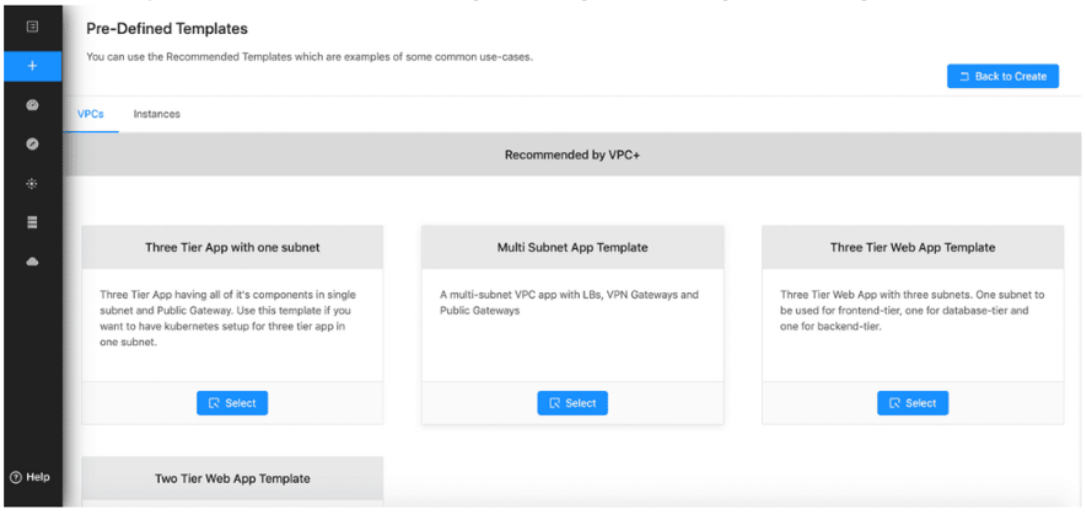
To create your VPC using pre-defined templates:

1. Go to the sidebar and click on Create. Then select Pre-Defined Templates.



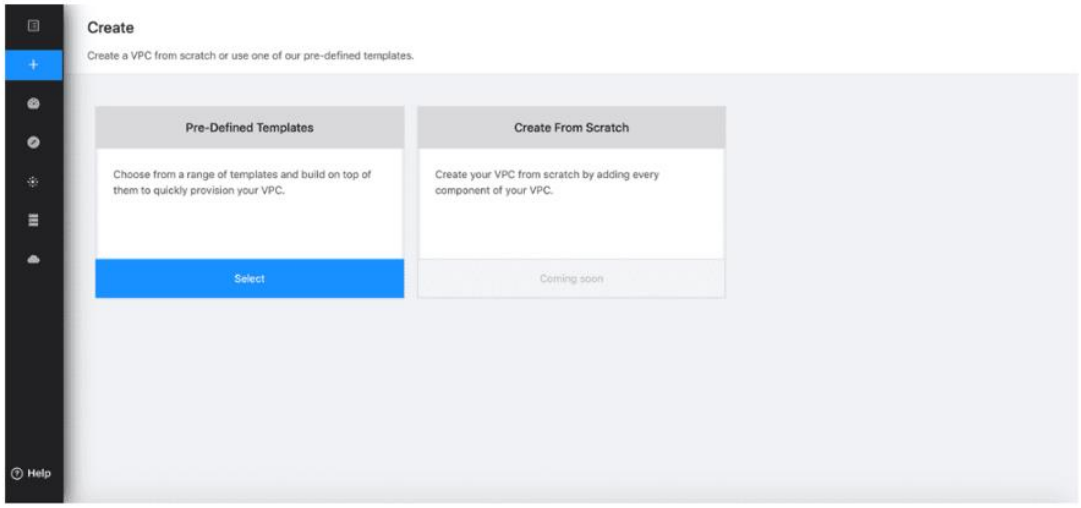
These are the templates used to create VPC

2. You can choose a template like **Two-Tier Web App, Three Tier Web App**, or **Three Tier App** with **One Subnet**. A template will create the structure for you where you can modify and make it your own.



To create a VPC from scratch:

1. Go to the sidebar, and click on Create.
2. Once there, select the Create From Scratch option to get started with your VPC workspace.



This is for to create a VPC from scratch.

Now see the virtual servers use in recovery and backup process

Backup strategies for IBM Power Systems Virtual Servers

Last updated 2023-07-07

Learn more about different AIX and IBM i backup strategies for IBM® Power Systems™ Virtual Server.

Image capture

Image capture produces a storage FlashCopy of the logical partition (LPAR) and works on both AIX, Linux, and IBM i LPARs. You can use image capture to store VM images within your account (locally) as a part of your image catalog, or directly to IBM Cloud Object Storage, or both.

Importing and exporting images requires a considerable amount of processing power and network bandwidth. As a result, you can submit only one import or export request before it is queued. Typically, users import or export system disks (AIX rootvg disks) that are smaller in size (**less than 1 TB**) to facilitate the transfer to and from Cloud Object Storage. If your image size is greater than 1 TB, your transfer might take a long time and is prone to failure. The maximum image size that you can import or export is **10 TB**.

AIX backup strategies

Power Systems Virtual Server users can implement any compatible agent-based backup for AIX virtual machines (VM). *Veeam for AIX* and *IBM Spectrum Protect* are two commonly used backup strategies.

- *Veeam for AIX* - See Additional backup strategies for more information.
- *IBM Spectrum Protect* provides scalable data protection for physical file servers, applications, and virtual environments. Organizations can scale up to manage billions of objects per backup server. They can reduce backup infrastructure costs with built-in data efficiency capabilities and the ability to migrate data to tape, public cloud services, and on-premises object storage. *IBM Spectrum Protect* can also be a data offload target for *IBM Spectrum Protect Plus*, for a long-term data retention and disaster recovery. For more information, see What can IBM Spectrum Protect do for your business? .

All these are the steps for backup strategies using virtual servers

It's the user's responsibility to set up and maintain these environments. Remember to check for any connectivity and bandwidth restrictions to the LPAR server. Your LPAR servers can also use IBM Cloud Object Storage as a repository.

For a complete tutorial on backing up and restoring AIX VM data, see Backing up and restoring data in an AIX VM .

For best practices and guidelines on AIX backup performance on IBM Power Systems Virtual Server, see AIX Backup Performance Best Practices and Guidelines on IBM Power Systems Virtual Server .

IBM i backup strategies

A common IBM i backup strategy is to use IBM® Backup, Recovery, and Media Services (BRMS) and IBM Cloud Storage Solutions (ICC). Together, these products automatically back up your LPARs to IBM Cloud Object Storage. The ICC product can be integrated with BRMS to move and retrieve objects from remote locations, including Cloud Object Storage. In most cases, this process involves backing up to virtual tapes and image catalogs. Note, you might need extra storage for the LPAR to host the image catalogs until they are moved to Cloud Object Storage.

The typical IBM i customer uses the following flow to back up LPARs and objects:

1. Use the 5733-ICC product to connect to Cloud Object Storage (COS) (~2 times the disk capacity to hold the backup images).
2. Connect to IBM COS by following the steps mentioned in Using Cloud Object Storage.
3. Complete the back up to COS by choosing the speed and resiliency that is required.
    - Working with ICC
    - BRMS with Cloud Storage Solutions for i considerations and requirements
    - Data backup and recovery by using BRMS and IBM Cloud Storage Solutions for i

For a complete tutorial on backing up and restoring IBM i VM data, see Backing up and restoring data in an IBM i VM .

Using Cloud Object Storage

The preferred way to connect to Cloud Object Storage (COS) from a VM in Power Systems Virtual Server are as follows:

1. In a PER workspace, attach the Power Systems Virtual Server workspace to a Transit Gateway and directly access the COS direct endpoint. See, Attaching Transit Gateway to a PER workspace.
2. In a non-PER workspace that are in a multi-zone region (MZR) the best way to connect to COS is as follows:
    a. Create a Virtual Private Cloud (VPC) with subnet(s) in the same region as your Power Systems Virtual Server workspace.
    b. Create a Virtual Private Endpoint gateway (VPE).
    c. Connect the VPC to a Transit Gateway.
    d. Create a cloud connection to connect the non-PER Power Systems Virtual Server workspace to the same transit gateway.

    The Power Systems Virtual Server would then use the VPE's IP address to connect to COS. If the VPE has multiple IP addresses, you can set up custom DNS and a custom hostname to connect to COS.
3. Deploy a Nginx reverse proxy server in either the classic or VPC infrastructure.

    Nginx is a mature, compact, and fast open source web server that excels at specialized tasks, including the reverse proxy server role. For information on setting up a Nginx reverse proxy server, see Installing your Nginx reverse proxy.

Here we use the cloud object storage

This is cloud AIX

Cloud Object Storage on AIX

IBM Power Systems that are running AIX 7.2 TL3, or later, have a script that is located in the path, `/usr/samples/nim/cloud_setup`. The `cloud_setup` command installs the command-line environment for cloud storage services.

```
cloud_setup [-I | G | C] [-v]

-I: Install the necessary RPMs for universal CLI (supports COS).
-G: Install the necessary RPMs for gsutil CLI (Google Cloud Storage).
-C: Install the necessary RPMs for cloud-init.
-v: Enable debug output.
```

1. To begin, copy the file to the system that requires AWS and give it execute permission.
2. Enter the `cloud_setup -I` command to install the AWS CLI and all of the dependant RPMs.
3. After the installation is complete, you must configure `awscli` for access to COS and provide the correct region (where your bucket COS is defined) in the `aws --endpoint-url` s3 command. In the following example, the **us-east** region is used:

```
# export PATH=$PATH:/opt/freeware/bin

# aws configure
AWS Access Key ID [None]: d197axxxxxxxxxxxxxxxxxxxxxxxxxxxa4
AWS Secret Access Key [None]: f52a5xxxxxxxxxxxxxxxxxxxxxxx001a33b74d8
Default region name [None]: us-east
Default output format [None]: json

# aws --endpoint-url https://s3.us-east.cloud-object-storage.appdomain.cloud s3 ls
2019-01-28 13:32:40 poweriaastest

# aws --endpoint-url https://s3.us-east.cloud-object-storage.appdomain.cloud s3 ls
s3://poweriaastest
2019-01-28 13:33:42 6832 nimstat.sh
2019-01-28 15:05:25 1380725 yum-3.4.3-5.aix6.1.noarch.rpm
```

Additional backup strategies

The additional backup strategies that you can use are as follows:

- FalconStor StorSafe VTL - For more information see FalconStor StorSafe VTL.
- Veeam for AIX - It provides simple physical server backup solutions for machines that are running in respective UNIX® operating systems. With them, IT organizations can provide industry-leading file-based backup and disaster recovery for their environments. For more information, see Veeam Agents for IBM AIX.

Ordering Veeam standalone licenses

You can order a Veeam® standalone license, via IBM Cloud portal Order Veeam Licesne

An email will be sent confirming the order. Should the order be incorrect, it can be deleted. For more information, see Managing Veeam licenses.

A license key will be generated and emailed to whomever placed the order.

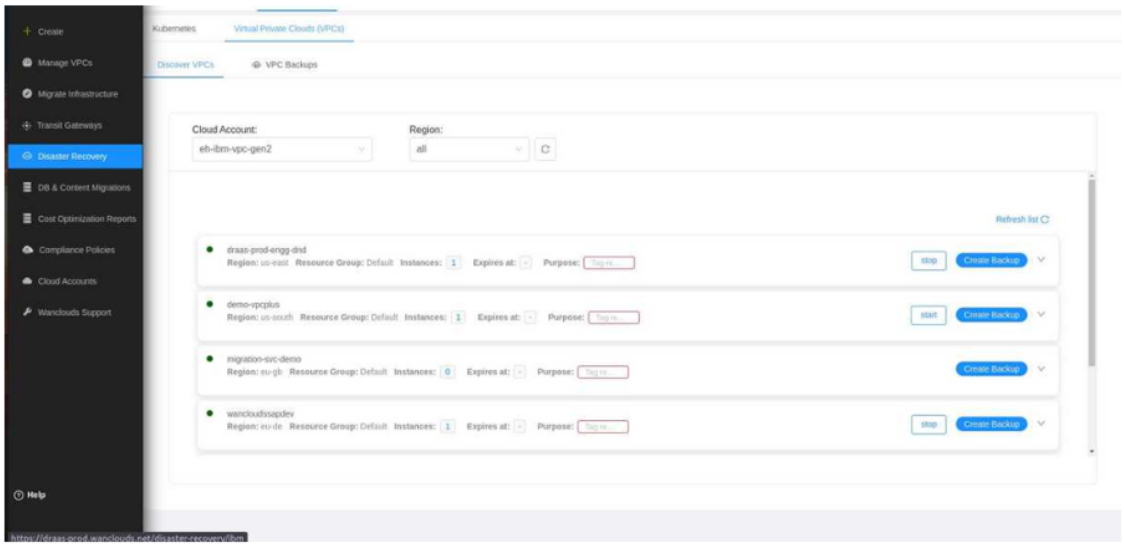
Managed services and IBM resiliency services

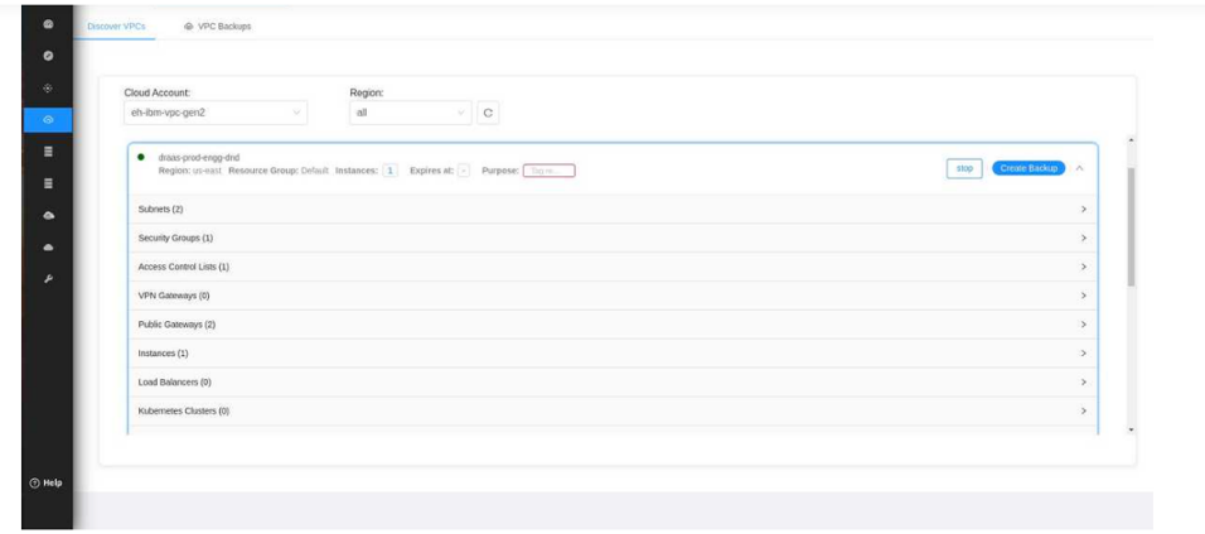
Contact an IBM representative if you need help with understanding the different backup lifecycle processes.

Backup using VPCs

Taking a backup of your VPCs

To Discover & Backup your VPC, navigate to Disaster Recovery from the side menu and select Discover VPCs tab.





Next, select the VCP you want to backup and click on Create Backup. Give your backup a Name and click Backup.

You can backup your Vpc from the following ways:

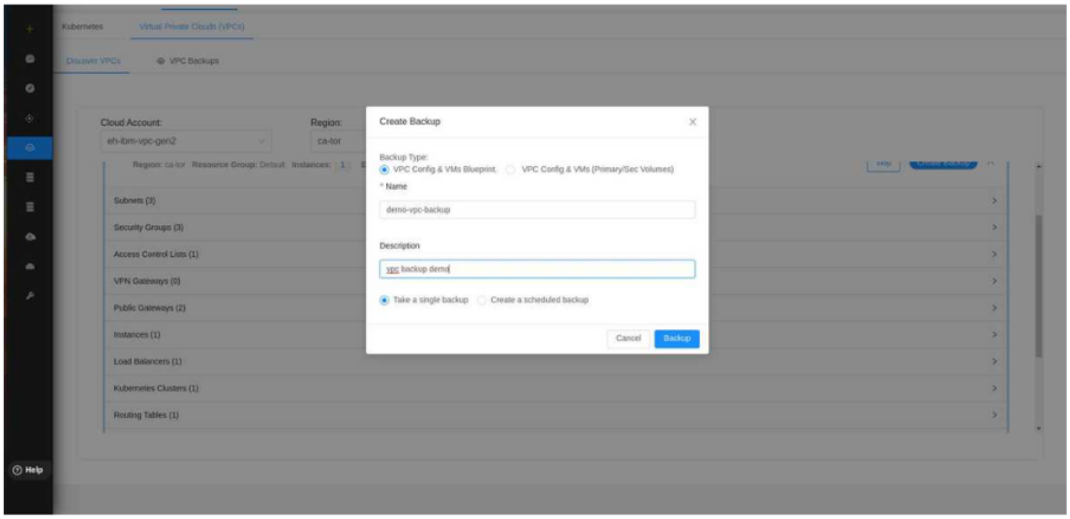
1) VPC Config & VMs Blueprint.

2) VPC Config & VMs (Primary/Sec Volume)

3) Schedule Recurring Backup

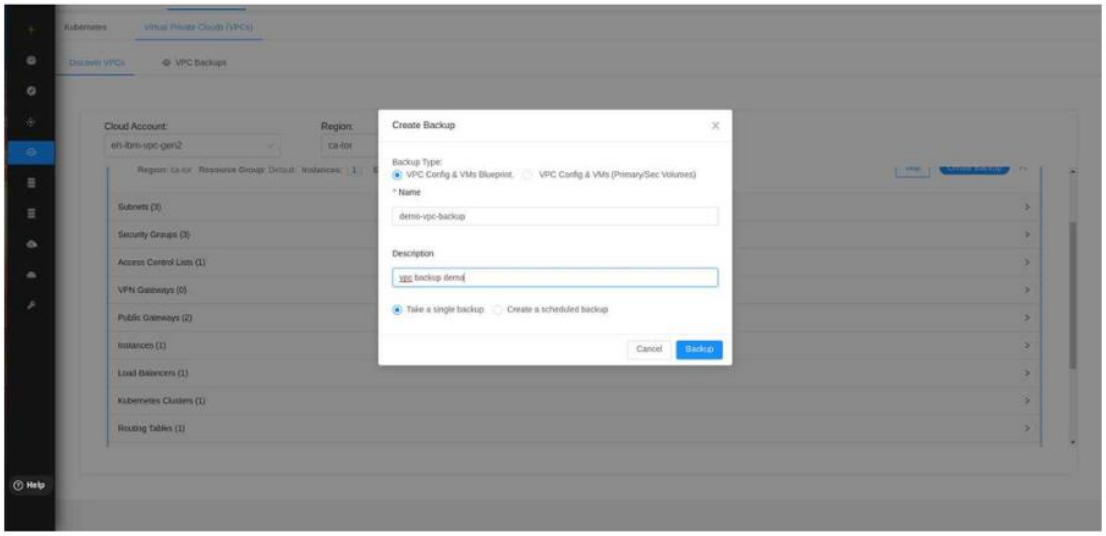
VPC Config & VMs Blueprint

If you want to take the VPC backup without the secondary volume (data) with instances then select this option.



VPC Config & VMs (Primary/Sec Volume)

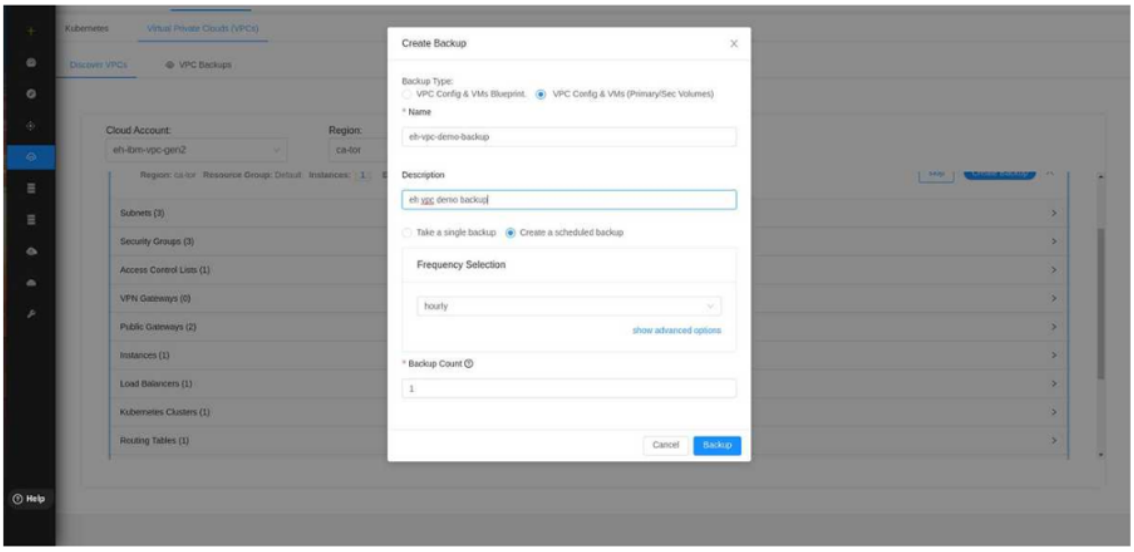
If you want to take a backup with all the secondary volume (data) with virtual server instances then select this option with all other resources.

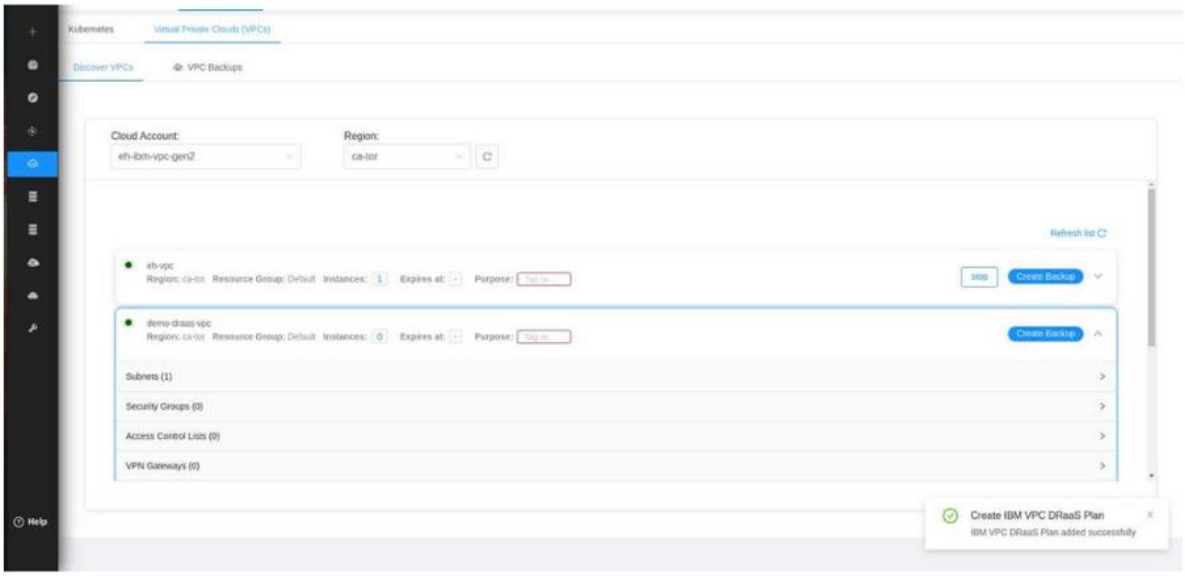


Schedule Recurring Backup

You can schedule backup operations so that the backups are initiated automatically at regular intervals. It allows you to schedule backups on an hourly, daily, weekly, monthly, annually or one-time basis.

You can also select the backup count in the specified time.

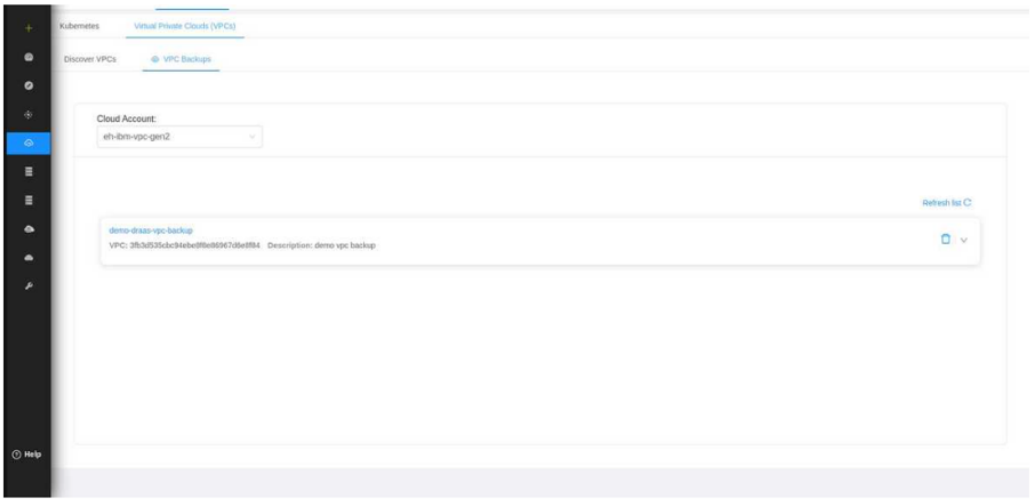


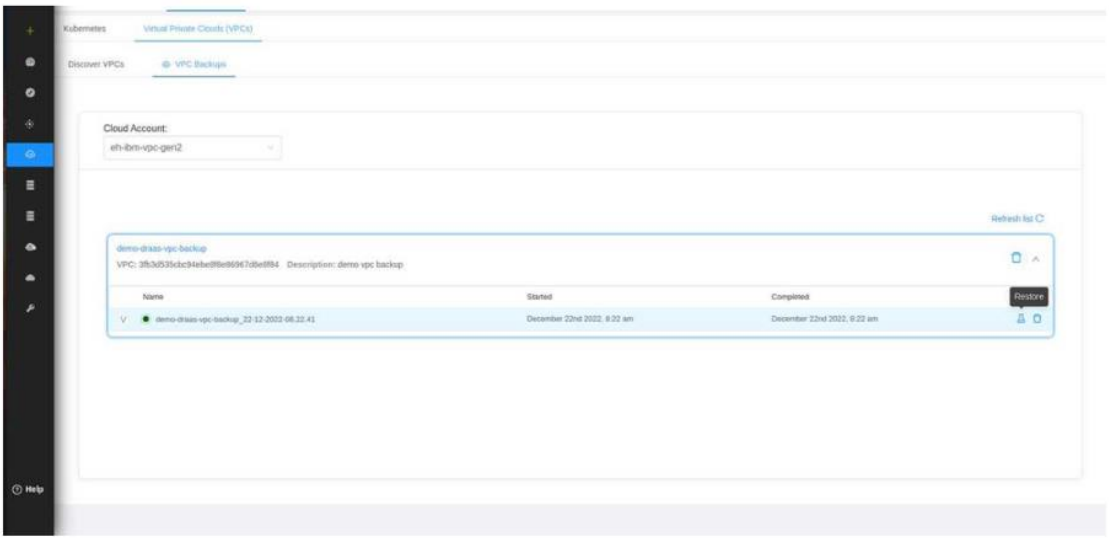


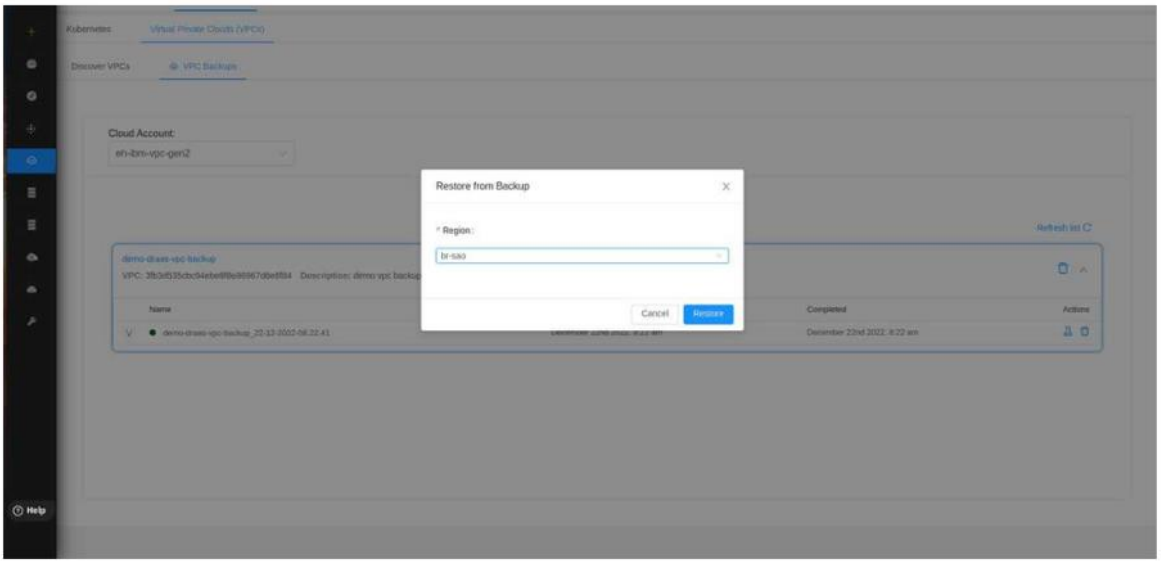
Restoring Process using VPCs

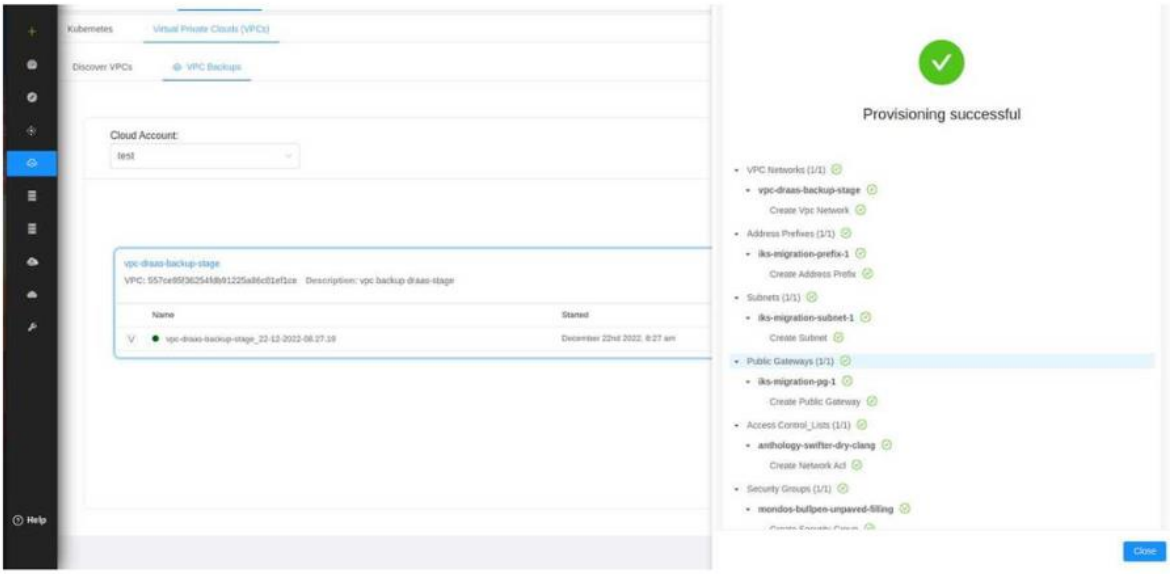
Restoring your VPCs

To restore resources from a VPC backup, go to the "VPCs Backups" tab, select the relevant cloud account, and view all available backups for the VPCs in that environment.









All these steps are about the testing, backup and recovery using the virtual servers and VPC with cloud .