

# 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.

The screenshot shows the Wanclouds website's sign-up interface. On the left, there is a diagram titled "Disaster Recovery as a Service" illustrating a workflow: "Backup & Restore VPC network design & functions, Kubernetes, OpenShift, Data and more" leads to "VPC", which then leads to "MaaS". The right side of the page is a "Sign Up" form. It includes input fields for "Full Legal Name", "Email", "Password", and "Confirm Password". Below these fields is a checkbox for "I agree to the Terms and Conditions and Privacy Policy". A "Register" button is positioned below the checkbox. At the bottom of the form, there is a link for "Already have an account? Login". The footer of the page states "© 2021, Wanclouds All Rights Reserved."

# Adding your cloud accounts

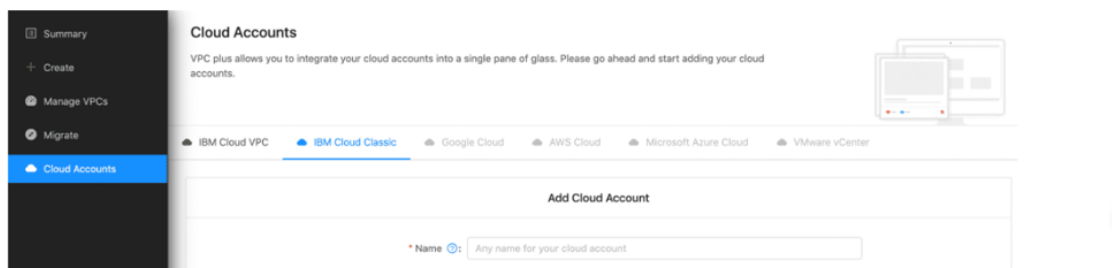
You must add a cloud account for VPC+ to be able to discover your existing environment. Adding a cloud account on VPC+ will let you:

- 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

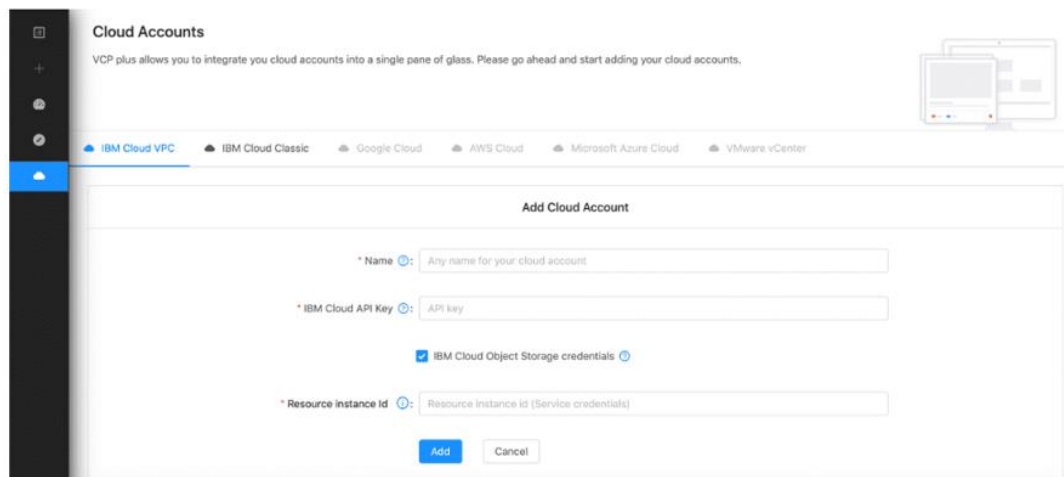
1. Navigate to the sidebar and click on **Cloud Accounts**.
2. Under the **IBM Cloud Classic** tab, click on **Add Account** to add your **Cloud account**.



The screenshot shows the 'Cloud Accounts' section of the VPC+ interface. The left sidebar has 'Cloud Accounts' selected. The main area has tabs for 'IBM Cloud VPC' and 'IBM Cloud Classic', with 'IBM Cloud Classic' being active. Below the tabs is the 'Add Cloud Account' form. The form has a single input field labeled '\* Name' with a placeholder 'Any name for 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)**.



The screenshot shows the 'Cloud Accounts' section of the VPC+ interface. The left sidebar has 'Cloud Accounts' selected. The main area has tabs for 'IBM Cloud VPC' and 'IBM Cloud Classic', with 'IBM Cloud VPC' being active. Below the tabs is the 'Add Cloud Account' form. The form has three input fields: '\* Name' (placeholder: 'Any name for your cloud account'), '\* IBM Cloud API Key' (placeholder: 'API key'), and '\* Resource instance id' (placeholder: 'Resource instance id (Service credentials)'). There is a checkbox labeled 'IBM Cloud Object Storage credentials' which is checked. At the bottom of the form are 'Add' and 'Cancel' buttons.

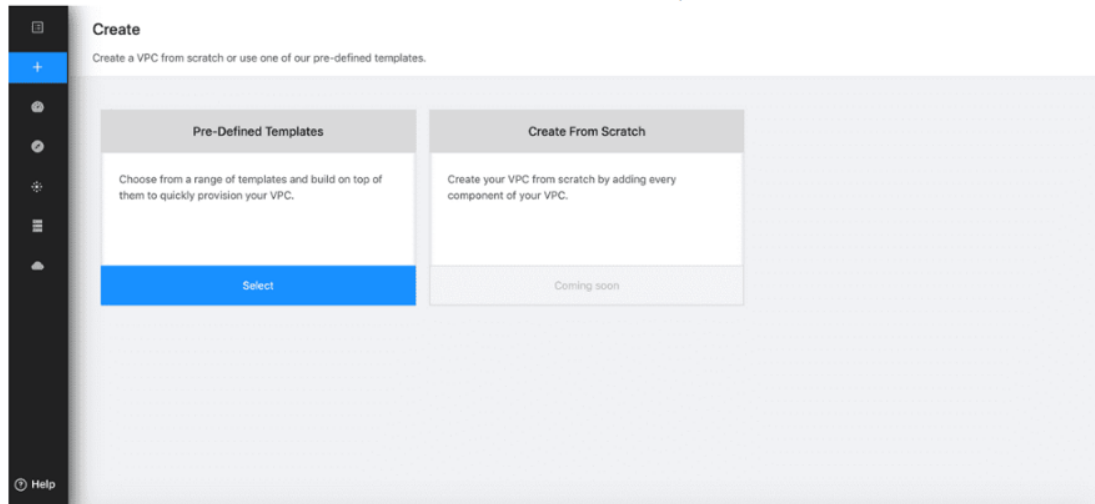
Here we give the API key and name then click on add the account will be added

# 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.

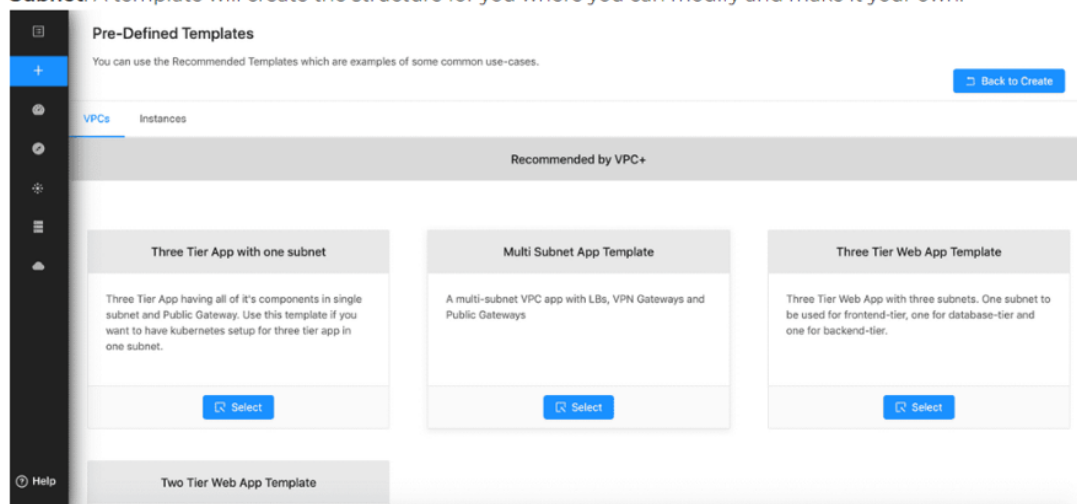
To create your VPC using pre-defined templates:

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



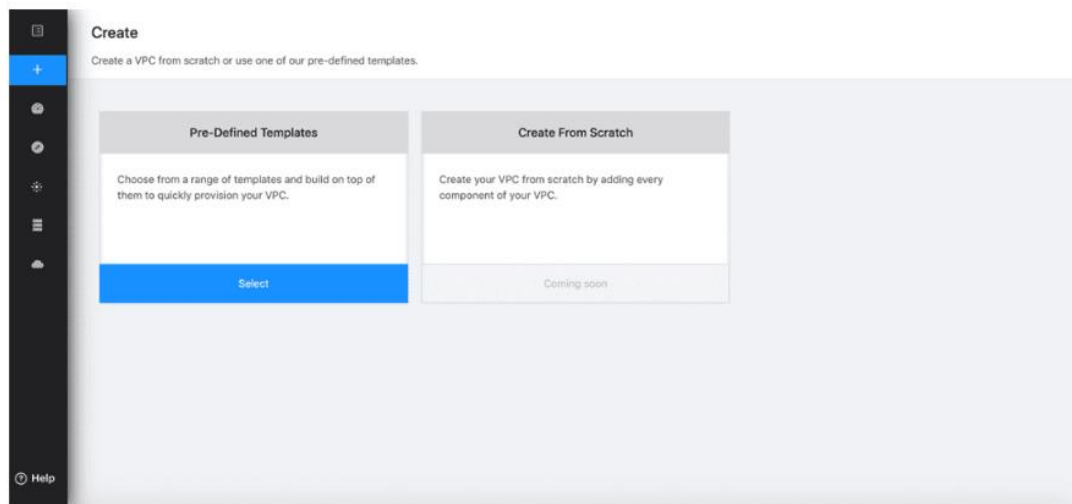
These are the templates used to create VPC

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]: d197axxxxxxxxxxxxxxxxxxxxxxxxxx4
AWS Secret Access Key [None]: f52a5xxxxxxxxxxxxxxxxxxxx001a33b74d8
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.

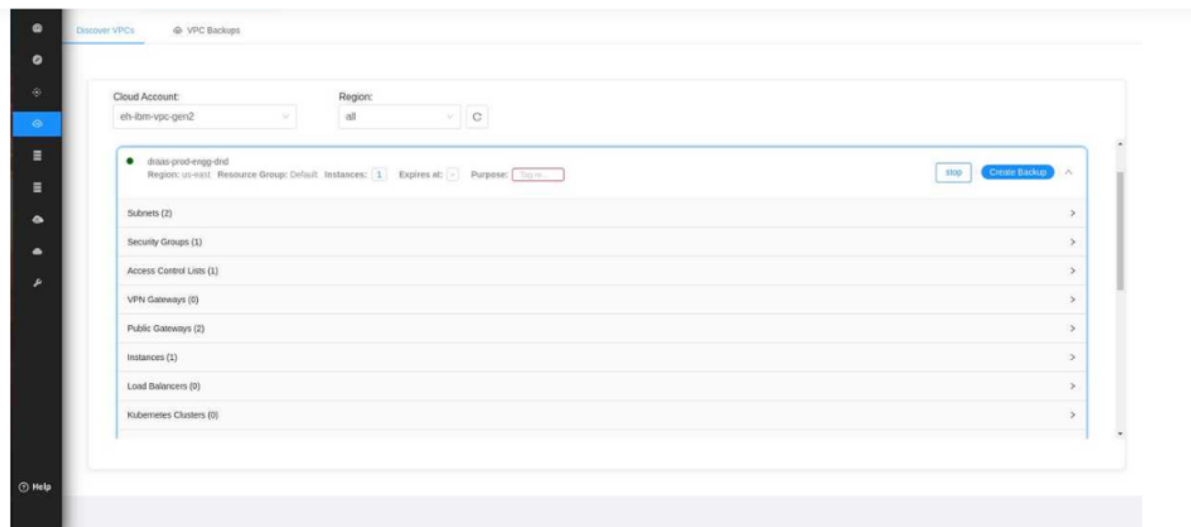
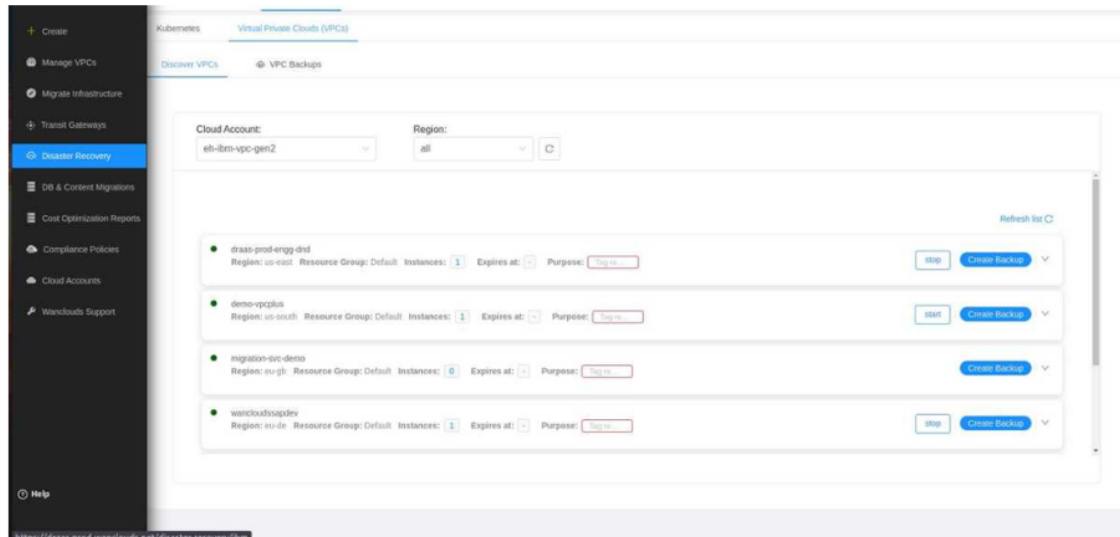
### Managed services and IBM resiliency services

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.

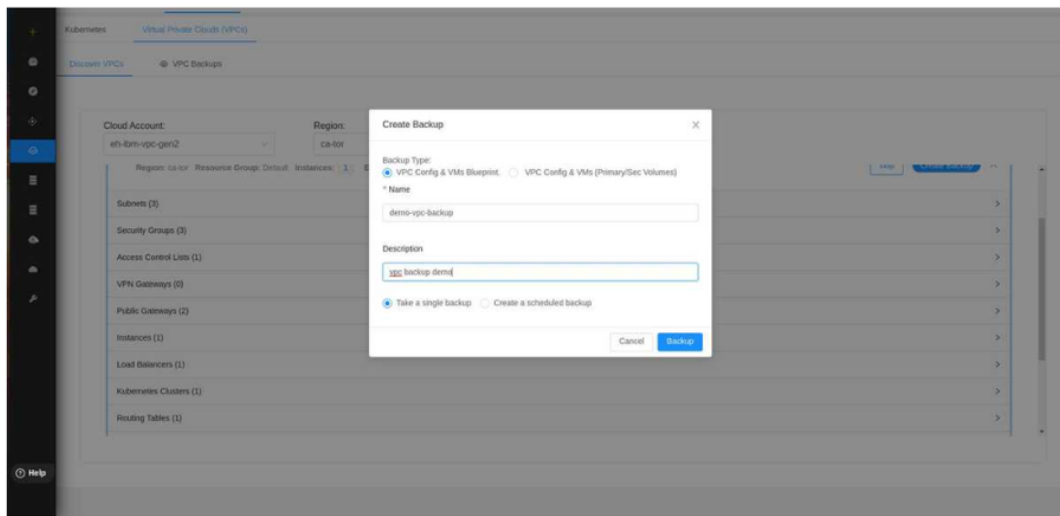
You can backup your Vpc from the following ways:

- 1) VPC Config & VMs Blueprint.
- 2) VPC Config & VMs (Primary/Sec Volume)
- 3) Schedule Recurring Backup



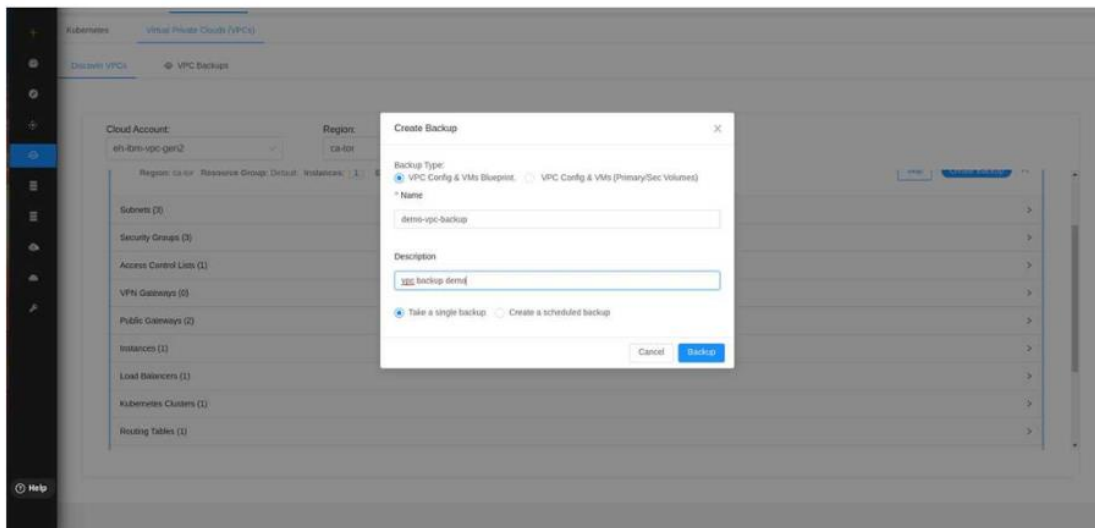
## VPC Config & VMs Blueprint

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)

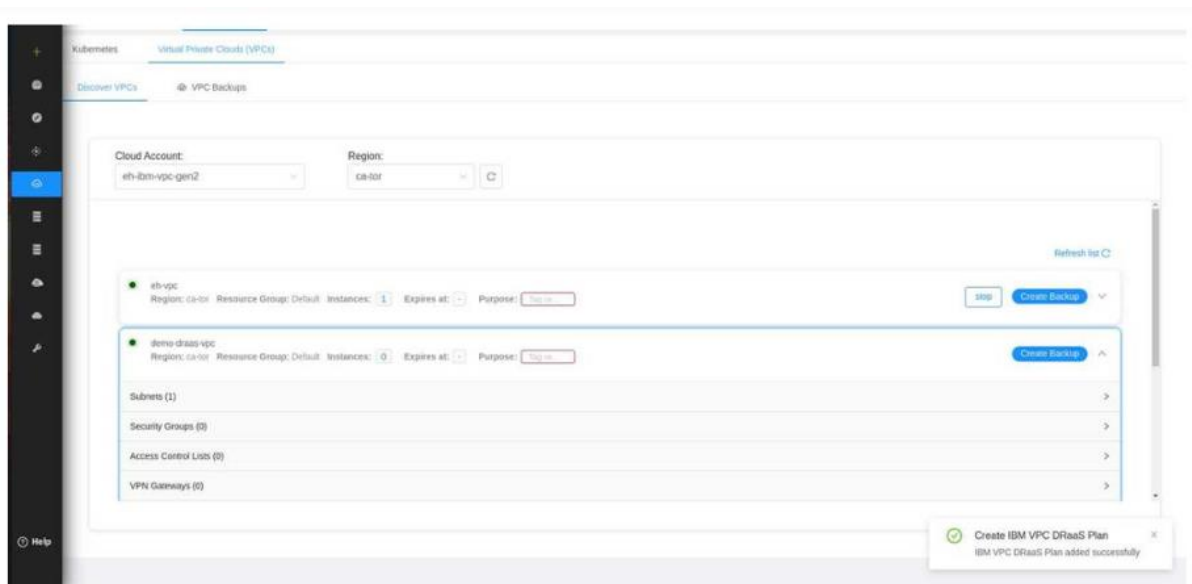
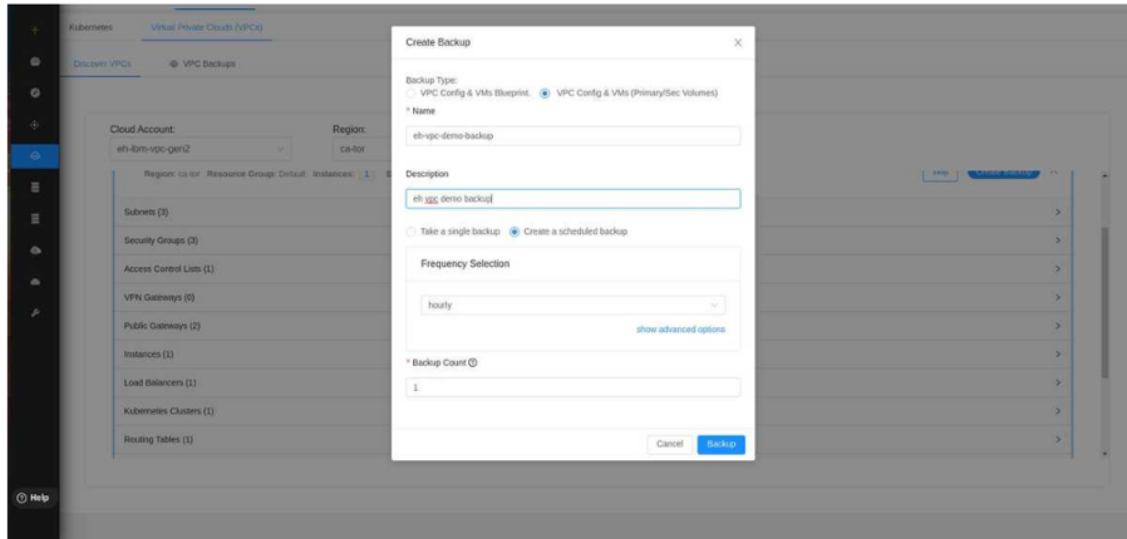
If you want to take a backup with all the secondary volume (data) with virtual server instances then select this option with all other resources.



## 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.

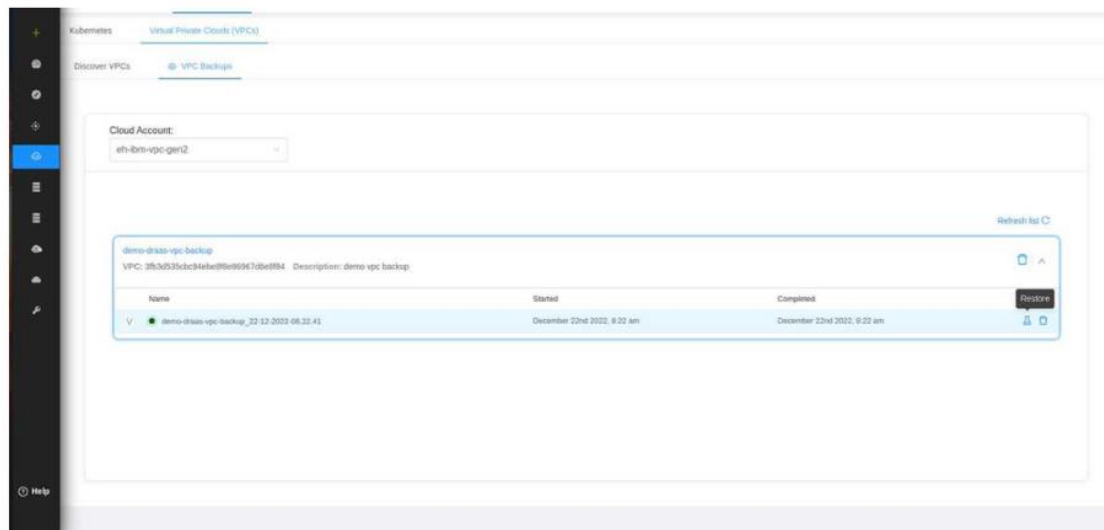
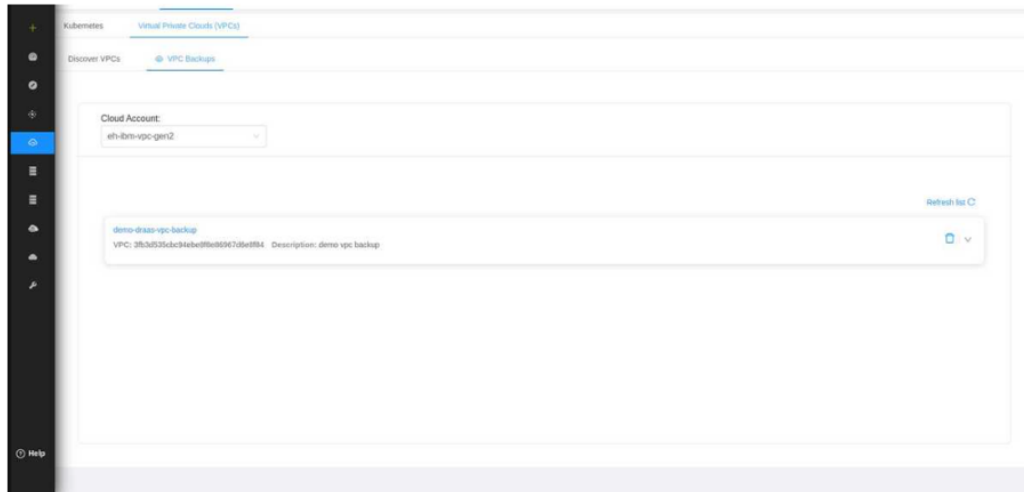
You can also select the backup count in the specified time.

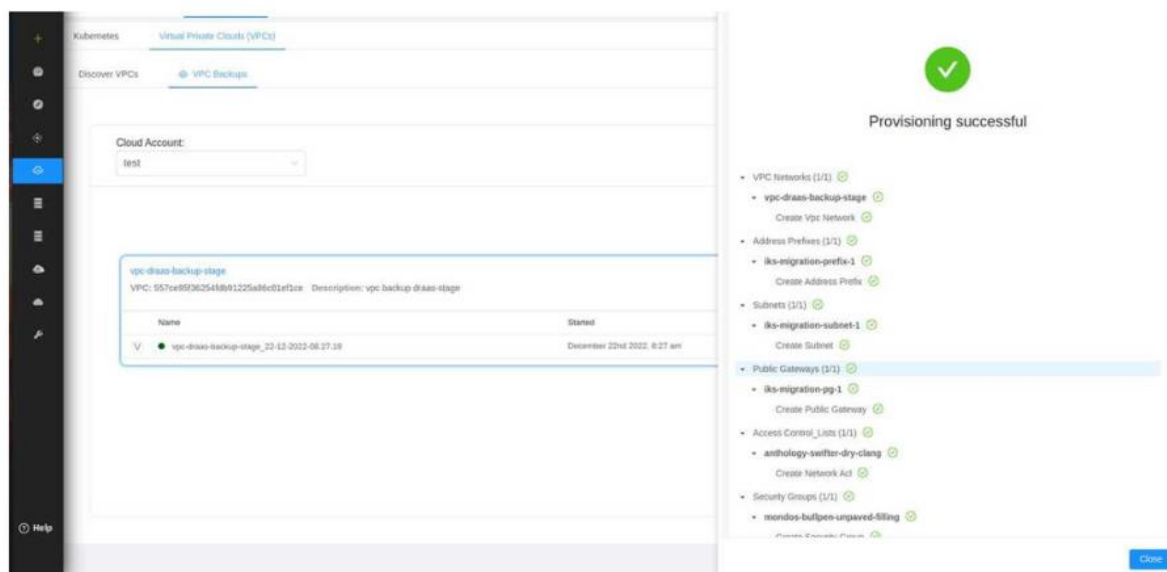
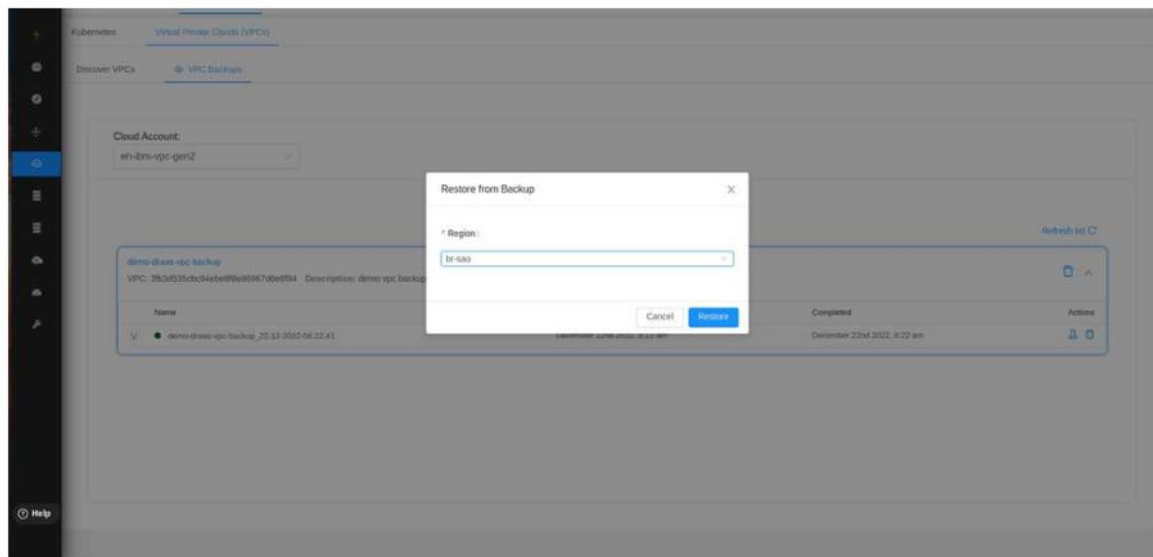


## Restoring Process using VPCs

# 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 .