Disaster Recovery with IBM Cloud Virtual Servers

PHASE 1

PROBLEM DEFINITION:

Disaster recovery (DR) is a crucial aspect of any IT infrastructure strategy, ensuring that your systems and data are protected and can be quickly restored in case of unexpected events or disasters. IBM Cloud offers a range of services and solutions to help you implement disaster recovery for your virtual servers. Here are the steps and considerations for setting up disaster recovery with IBM Cloud Virtual Servers.

PLATFORM DESIGN AND USER EXPERIENCE:

CHALLENGE: Design an intuitive and user-friendly platform that showcases artisanal products effectively.

SOLUTION: Invert in user-certered design, implement responsive web design, and conduct usability testing to ensure a seamless user experience.

1. Assessment and Planning:

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

Determine your Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO is the acceptable data loss, and RTO is the time it takes to recover your systems. Decide on the appropriate IBM Cloud data center or availability zone for your disaster recovery site.

2. IBM Cloud Virtual Servers:

Deploy your primary virtual servers in your chosen IBM Cloud region or availability zone.

3. Backup and Replication:

Use IBM Cloud Backup or another backup solution to regularly back up your virtual servers and data. Ensure backups are stored securely.

4. Replication Solution:

IBM Cloud offers solutions like IBM Hyper Protect Virtual Servers or third-party options for replicating your virtual servers and data to a secondary site. This secondary site should be in a different geographic location for better disaster recovery.

5. Network Configuration:

Set up a secure, high-speed network connection between your primary and secondary data centers or availability zones. IBM Cloud provides options like Direct Link for dedicated and reliable connectivity.

6. Failover and Testing:

Regularly test your disaster recovery setup to ensure it works as expected. Simulate failover scenarios to verify the recovery process.

Develop detailed runbooks and documentation for your DR procedures.

7. Monitoring and Automation:

Implement monitoring and alerting systems to detect issues in real-time.

Consider using automation tools or scripts to trigger failover procedures automatically when certain conditions are met.

8. Security and Compliance:

Ensure that security measures are in place to protect your data during replication and failover.

Comply with regulatory requirements relevant to your industry and location.

9. Documentation and Training:

Document your disaster recovery plan, including contact information, procedures, and responsibilities.

Train your team on the DR plan and conduct regular drills.

10. Regular Updates:

As your infrastructure and applications evolve, make sure your disaster recovery plan and systems are updated accordingly.

11. Cost Management:

Understand the cost implications of your disaster recovery setup and ensure it aligns with your budget.

12. Third-Party Solutions:

Consider third-party disaster recovery solutions that integrate with IBM Cloud if you need additional features or capabilities.

13. Compliance and Testing:

Ensure that your disaster recovery solution complies with industry standards and regulations.

Regularly test your DR plan to validate its effectiveness.

CONCLUSION:

Remember that disaster recovery is an ongoing process, and it's essential to periodically review and update your plan to meet changing business needs and technology advancements. IBM Cloud provides a robust infrastructure for implementing disaster recovery solutions, and working with their experts can help you design a solution tailored to your specific requirements.

DISASTER RECOVERY

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.

INTRODUCTION:-

Uptime is a key client expectation for IBM i workloads. Across geographic locations, this is accomplished with a disaster recovery (DR) solution. IBM Power Virtual Server (PowerVS) meets that requirement by enabling clients to leverage DR solutions between two IBM i Virtual Server Instances (VSIs) in separate IBM Cloud datacenters.

An important characteristic of DR solutions for PowerVS is that they are based on logical or operating system-level replication. Many Power Systems clients today use storage-based replication for DR, which is not an option with PowerVS.

This document will provide step-by-step instructions to accomplish both phases of configuring DR for IBM i workloads in PowerVS:-

1. Performing the required network configuration.

2. Implementing the DR solution itself.

USE CASES:-

PowerHA Geographic Mirroring:-

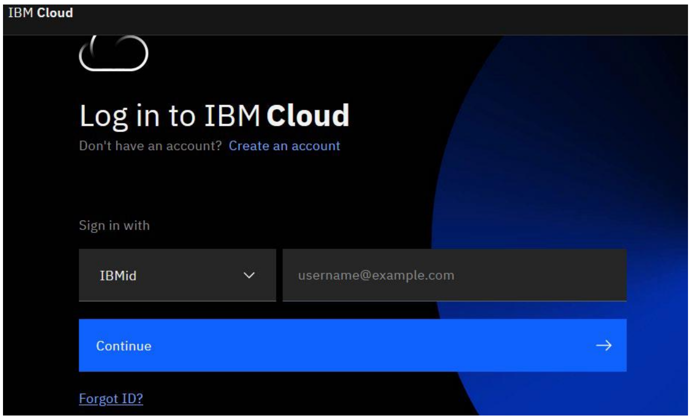
In this case we will demonstrate how to implement PowerHA Geographic Mirroring in IBM i, which provides DR by using operating system (OS) clustering and replication. This solution requires that the IBM i VSI and client application(s) use Independent Auxiliary Storage Pools (IASPs). If the IBM i VSI and application(s) use only *SYSBAS, this DR option will not work

CREATING DB2 AND COGNO SERVICE ON OUR IBM CLOUD ACCOUNT:-

After we creating a Lite account (Trail Free account) as a student. Login to IBM cloud.

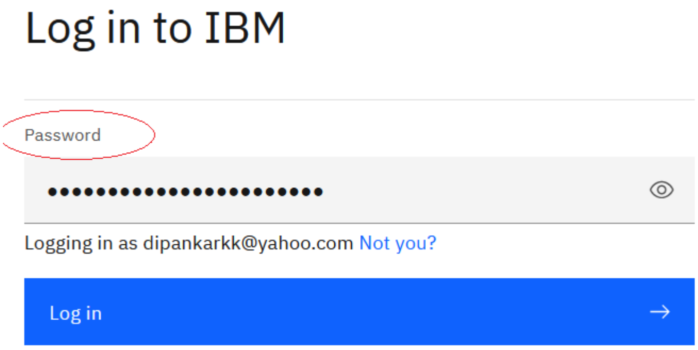
https://cloud.ibm.com/login

Enter your registered mail id.



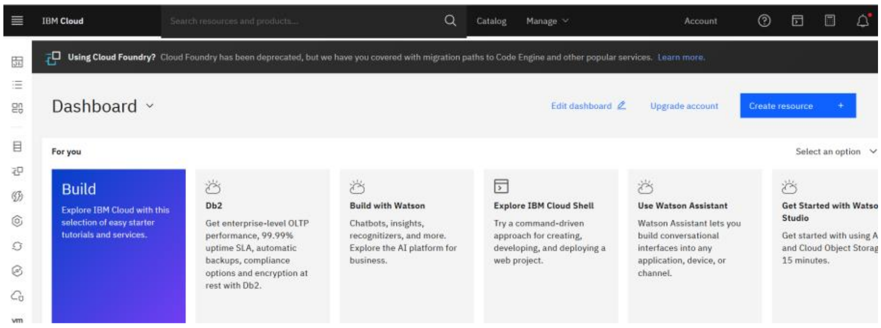
Then Enter **Password**

LOGIN TO IBM:-



Logging in as dipankarkk@yahoo.com Not you?

Aftser successfully login, user will be redirected to account Dashboard page.



Using Cloud Foundry? Cloud Foundry has been deprecated, but we have you covered with migration paths to Code Engine and other popular services. Learn more.

Build
Explore IBM Cloud with this selection of easy starter tutorials and services.

Db2
Get enterprise-level OLTP performance, 99.99% uptime SLA, automatic backups, compliance options and encryption at rest with Db2.

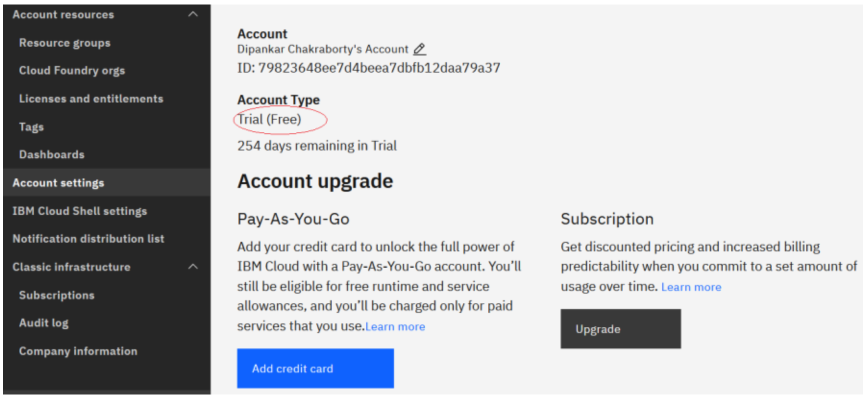
Build with Watson
Chatbots, insights, recognitizers, and more. Explore the AI platform for business.

Explore IBM Cloud Shell
Try a command-driven approach for creating, developing, and deploying a web project.

Use Watson Assistant
Watson Assistant lets you build conversational interfaces into any application, device, or channel.

Get Started with Watso Studio
Get started with using A and Cloud Object Storag 15 minutes.

ACCOUNT SETTING:-



Account
Dipankar Chakraborty's Account
ID: 79823648ee7d4beea7dbfb12daa79a37

Account Type
Trial (Free)
254 days remaining in Trial

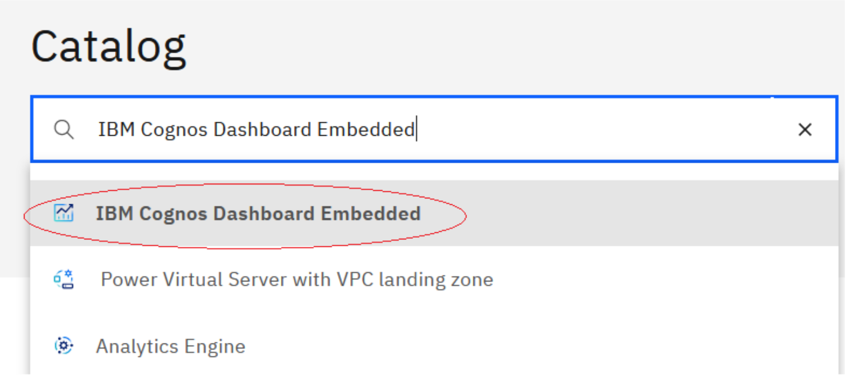
Account upgrade

Pay-As-You-Go
Add your credit card to unlock the full power of IBM Cloud with a Pay-As-You-Go account. You'll still be eligible for free runtime and service allowances, and you'll be charged only for paid services that you use. Learn more

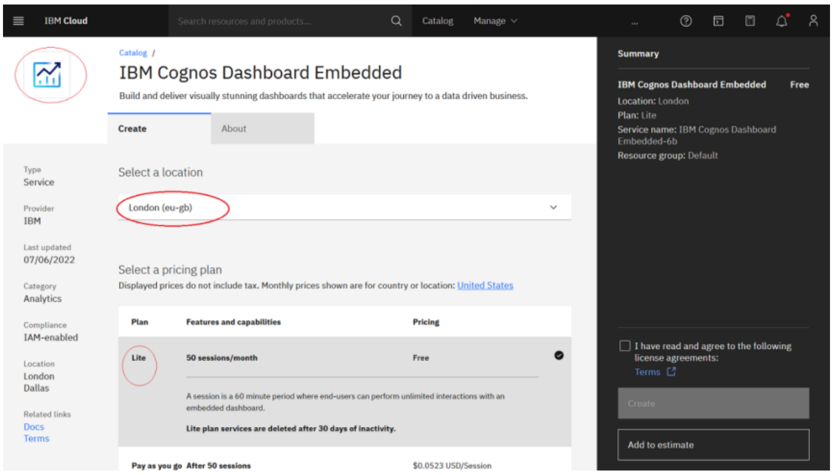
Subscription
Get discounted pricing and increased billing predictability when you commit to a set amount of usage over time. Learn more

Add IBM Cognos Dashboard Embedded service in your account:-

Click on **Catalog** menu on top page. Then enter Cognos in search box.


Catalog
IBM Cognos Dashboard Embedded
IBM Cognos Dashboard Embedded
Power Virtual Server with VPC landing zone
Analytics Engine

Click "IBM Cognos Dashboard Embedded", it will redirect you to Cognos page. Once you are on Cognos page.



IBM Cognos Dashboard Embedded
Build and deliver visually stunning dashboards that accelerate your journey to a data driven business.

Type: Service
Provider: IBM
Last updated: 07/06/2022
Category: Analytics
Compliance: IAM-enabled
Location: London, Dallas

Select a location
London (eu-gb)

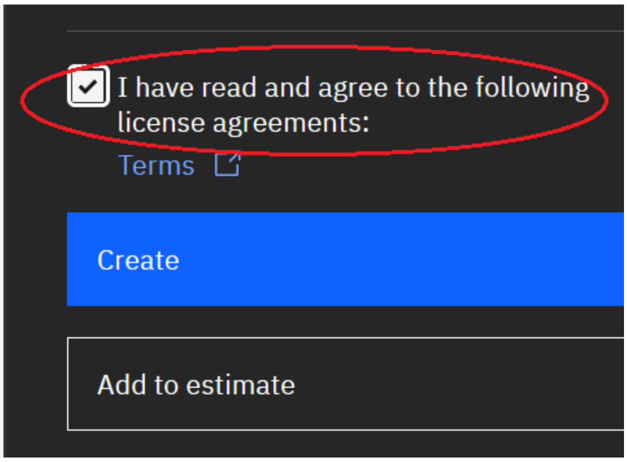
Select a pricing plan
Displayed prices do not include tax. Monthly prices shown are for country or location: United States

Plan	Features and capabilities	Pricing
Lite	50 sessions/month A session is a 60 minute period where end-users can perform unlimited interactions with an embedded dashboard. Lite plan services are deleted after 30 days of inactivity.	Free
Pay as you go	After 50 sessions	$0.0523 USD/Session

Summary
IBM Cognos Dashboard Embedded — Free
Location: London
Plan: Lite
Service name: IBM Cognos Dashboard Embedded-6b
Resource group: Default

□ I have read and agree to the following license agreements: Terms

Select a Location: **London**
Select a pricing plan: **Lite**.
Select terms & condition (license agreements)

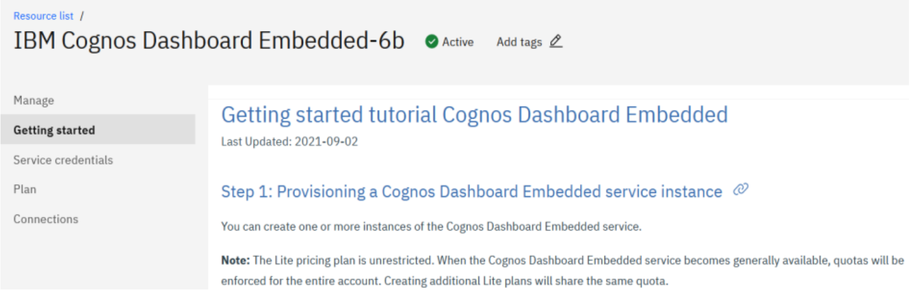


☑ I have read and agree to the following license agreements:

Terms

Then click on **Create** buton.
After you click on create, it will take some time to create the service.

user will be redirect to Cognos tutorial page.



Getting started tutorial Cognos Dashboard Embedded

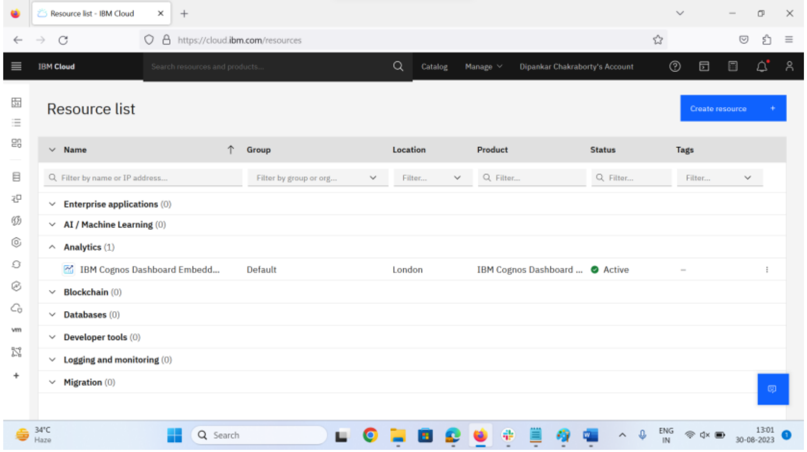
Last Updated: 2021-09-02

Step 1: Provisioning a Cognos Dashboard Embedded service instance

You can create one or more instances of the Cognos Dashboard Embedded service.

Note: The Lite pricing plan is unrestricted. When the Cognos Dashboard Embedded service becomes generally available, quotas will be enforced for the entire account. Creating additional Lite plans will share the same quota.

It takes few minutes to service created at cloud account. After few minutes you can check resource list.

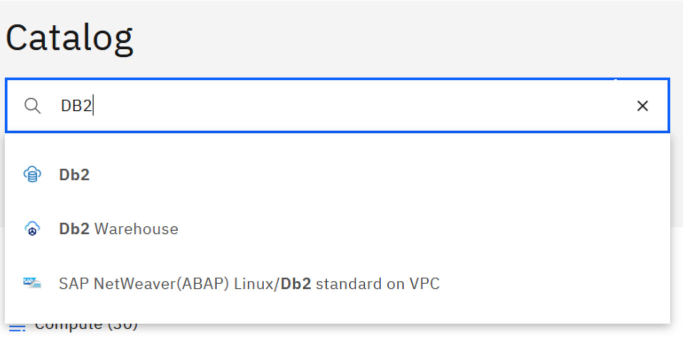


Resource list - IBM Cloud
https://cloud.ibm.com/resources
IBM Cloud
Search resources and products...
Catalog
Manage
Dipankar Chakraborty's Account
Create resource
34°C
Haze
Search
ENG
IN
13:01
30-08-2023

Resource list

Name	Group	Location	Product	Status	Tags
Enterprise applications (0)					
AI / Machine Learning (0)					
Analytics (1)					
IBM Cognos Dashboard Embedd...	Default	London	IBM Cognos Dashboard ...	Active	–
Blockchain (0)					
Databases (0)					
Developer tools (0)					
Logging and monitoring (0)					
Migration (0)					

Now again search DB2 on catalog



Catalog

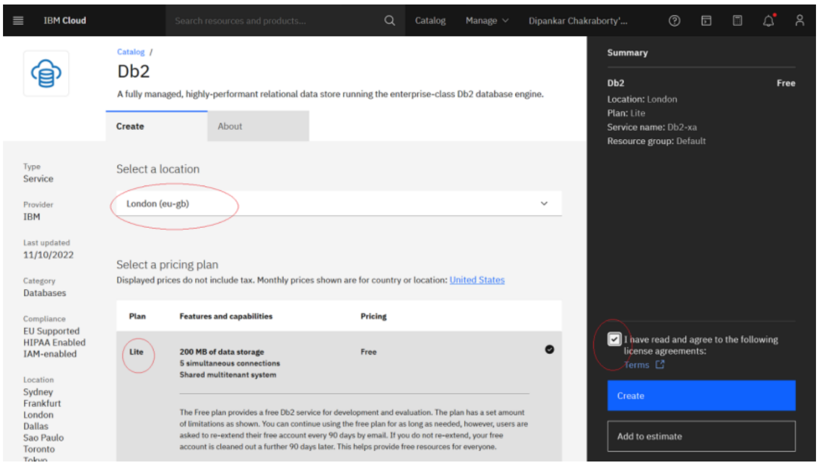
DB2

Db2

Db2 Warehouse

SAP NetWeaver(ABAP) Linux/Db2 standard on VPC

Click on Db2, you will be redirect to DB2 service page.



Catalog /

Db2

A fully managed, highly-performant relational data store running the enterprise-class Db2 database engine.

Type
Service

Provider
IBM

Last updated
11/10/2022

Category
Databases

Compliance
EU Supported
HIPAA Enabled
IAM-enabled

Location
Sydney
Frankfurt
London
Dallas
Sao Paulo
Toronto
Tokyo

Select a location

London (eu-gb)

Select a pricing plan

Displayed prices do not include tax. Monthly prices shown are for country or location: United States

Plan	Features and capabilities	Pricing
Lite	200 MB of data storage 5 simultaneous connections Shared multitenant system	Free

The Free plan provides a free Db2 service for development and evaluation. The plan has a set amount of limitations as shown. You can continue using the free plan for as long as needed, however, users are asked to re-extend their free account every 90 days by email. If you do not re-extend, your free account is cleaned out a further 90 days later. This helps provide free resources for everyone.

Summary

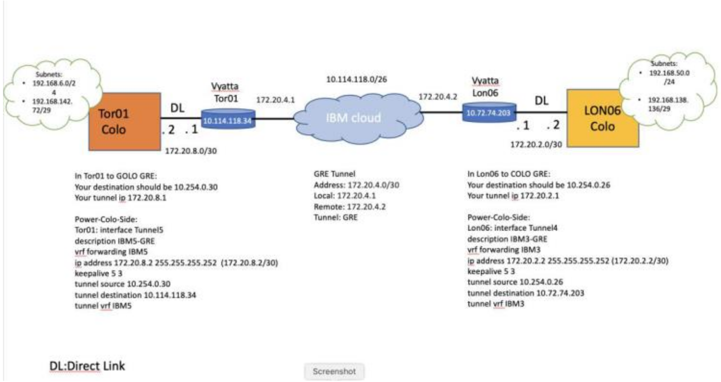
Db2 Free
Location: London
Plan: Lite
Service name: Db2-xa
Resource group: Default

☑ I have read and agree to the following license agreements:
Terms

Select a Location: **London**
Select a pricing plan: **Lite**.
Select terms & condition (license agreements)
Then click on **Create** buton.
After you click on create, it will take some time to create the service.

DIAGRAMS:-

The overall architecture of our deployment is shown below:-



```
In Tor01 to GOLO GRE:
Your destination should be 10.254.0.30
Your tunnel ip 172.20.8.1

Power-Colo-Side:
Tor01: interface Tunnel5
description IBM5-GRE
vrf forwarding IBM5
ip address 172.20.8.2 255.255.255.252  (172.20.8.2/30)
keepalive 5 3
tunnel source 10.254.0.30
tunnel destination 10.114.118.34
tunnel vrf IBM5
```

```
GRE Tunnel
Address: 172.20.4.0/30
Local: 172.20.4.1
Remote: 172.20.4.2
Tunnel: GRE
```

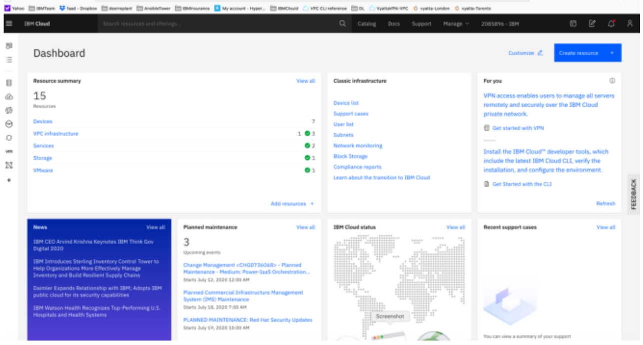
```
In Lon06 to COLO GRE:
Your destination should be 10.254.0.26
Your tunnel ip 172.20.2.1

Power-Colo-Side:
Lon06: interface Tunnel4
description IBM3-GRE
vrf forwarding IBM3
ip address 172.20.2.2 255.255.255.252 (172.20.2.2/30)
keepalive 5 3
tunnel source 10.254.0.26
tunnel destination 10.72.74.203
tunnel vrf IBM3
```

DL:Direct Link

Verify your Vyatta Gateway access:-

The Vyatta Gateway address can be find in the IBM Cloud UI under Devices.

Login to IBM Cloud UI and press “IBM Cloud” on top left-hand side.



Dashboard

Resource summary — View all

15
Resources

Devices	7
VPC infrastructure	1 ● 3
Services	● 2
Storage	● 1
VMware	● 1

Add resources +

Classic infrastructure

- Device list
- Support cases
- User list
- Subnets
- Network monitoring
- Block Storage
- Compliance reports
- Learn about the transition to IBM Cloud

For you

VPN access enables users to manage all servers remotely and securely over the IBM Cloud private network.

Get started with VPN

Install the IBM Cloud™ developer tools, which include the latest IBM Cloud CLI, verify the installation, and configure the environment.

Get Started with the CLI

Refresh

News — View all

IBM CEO Arvind Krishna Keynotes IBM Think Gov Digital 2020

IBM Introduces Sterling Inventory Control Tower to Help Organizations More Effectively Manage Inventory and Build Resilient Supply Chains

Daimler Expands Relationship with IBM; Adopts IBM public cloud for its security capabilities

IBM Watson Health Recognizes Top-Performing U.S. Hospitals and Health Systems

Planned maintenance — View all

3
Upcoming events

Change Management <CHG0736068> - Planned Maintenance - Medium: Power-IaaS Orchestration...
Starts July 12, 2020 12:00 AM

Planned Commercial Infrastructure Management System (IMS) Maintenance
Starts July 18, 2020 7:00 AM

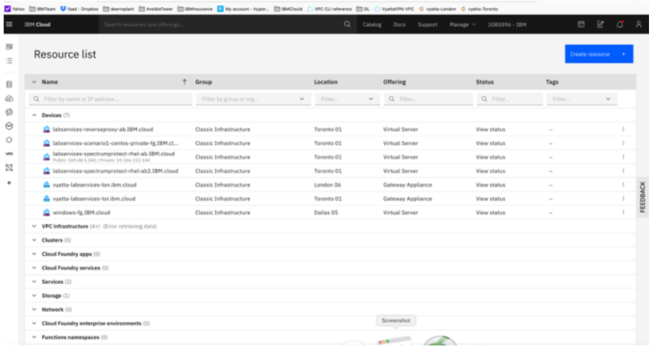
PLANNED MAINTENANCE: Red Hat Security Updates
Starts July 19, 2020 10:00 AM

IBM Cloud status — View all

Recent support cases — View all

You can view a summary of your support

Click on “Devices”



Resource list

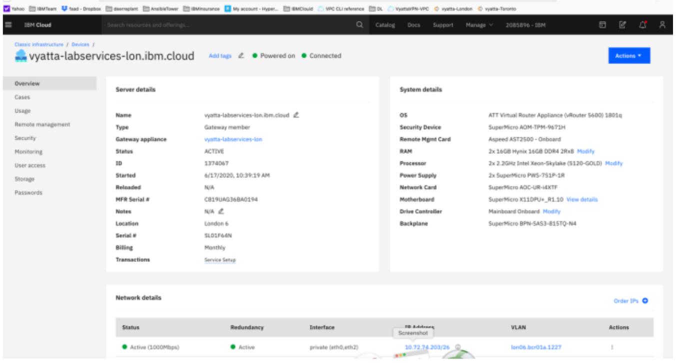
Name	Group	Location	Offering	Status	Tags
Filter by name or IP address...	Filter by group or org...	Filter...	Filter...	Filter...	Filter...
Devices (7)					
labservices-reverseproxy-ab.IBM.cloud	Classic Infrastructure	Toronto 01	Virtual Server	View status	–
labservices-scenario1-centos-private-fg.IBM.cl...	Classic Infrastructure	Toronto 01	Virtual Server	View status	–
labservices-spectrumprotect-rhel-ab.IBM.cloud Public: 169.48.5.242 / Private: 10.166.112.144	Classic Infrastructure	Toronto 01	Virtual Server	View status	–
labservices-spectrumprotect-rhel-ab2.IBM.cloud	Classic Infrastructure	Toronto 01	Virtual Server	View status	–
vyatta-labservices-lon.ibm.cloud	Classic Infrastructure	London 06	Gateway Appliance	View status	–
vyatta-labservices-tor.ibm.cloud	Classic Infrastructure	Toronto 01	Gateway Appliance	View status	–
windows-fg.IBM.cloud	Classic Infrastructure	Dallas 05	Virtual Server	View status	–
VPC infrastructure (4+) (Error retrieving data)					
Clusters (0)					
Cloud Foundry apps (0)					
Cloud Foundry services (0)					
Services (2)					
Storage (1)					
Network (0)					
Cloud Foundry enterprise environments (0)					
Functions namespaces (0)					

The Vyatta system we like to configure:-

vyatta-labservices-lon.ibm.cloud

LON06:-

Click on the London Vyatta: vyatta-labservices-lon.ibm.cloud



Classic infrastructure / Devices /

vyatta-labservices-lon.ibm.cloud   Add tags   ● Powered on   ● Connected

Server details

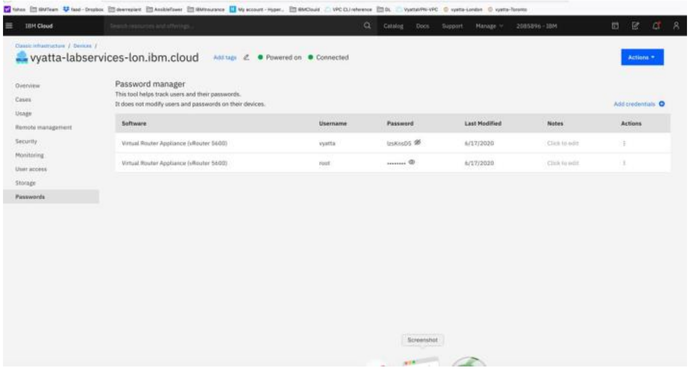
Name	vyatta-labservices-lon.ibm.cloud
Type	Gateway member
Gateway appliance	vyatta-labservices-lon
Status	ACTIVE
ID	1374067
Started	6/17/2020, 10:39:19 AM
Reloaded	N/A
MFR Serial #	C819UAG36BA0194
Notes	N/A
Location	London 6
Serial #	SL01F64N
Billing	Monthly
Transactions	Service Setup

System details

OS	ATT Virtual Router Appliance (vRouter 5600) 1801q
Security Device	SuperMicro AOM-TPM-9671H
Remote Mgmt Card	Aspeed AST2500 - Onboard
RAM	2x 16GB Hynix 16GB DDR4 2Rx8 Modify
Processor	2x 2.2GHz Intel Xeon-Skylake (5120-GOLD) Modify
Power Supply	2x SuperMicro PWS-751P-1R
Network Card	SuperMicro AOC-UR-i4XTF
Motherboard	SuperMicro X11DPU+_R1.10 View details
Drive Controller	Mainboard Onboard Modify
Backplane	SuperMicro BPN-SAS3-815TQ-N4

Network details

Status	Redundancy	Interface	IP Address	VLAN	Actions
● Active (1000Mbps)	● Active	private (eth0,eth2)	10.72.74.203/26	lon06.bcr01a.1227	⋮



IBM Cloud

Classic infrastructure / Devices /

vyatta-labservices-lon.ibm.cloud ● Powered on ● Connected

Overview
Cases
Usage
Remote management
Security
Monitoring
User access
Storage
Passwords

Password manager

This tool helps track users and their passwords.
It does not modify users and passwords on their devices.

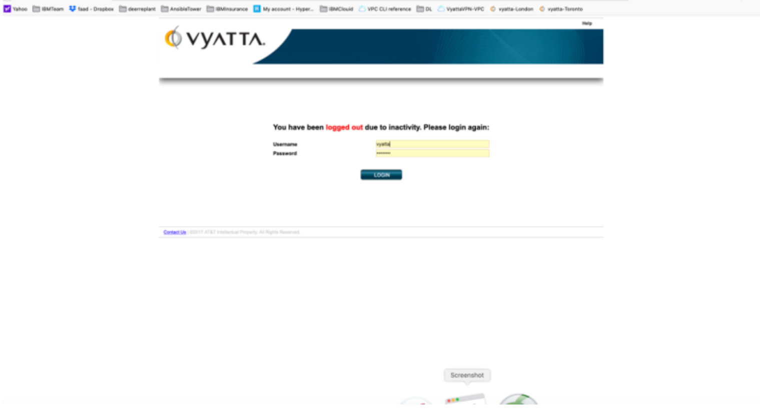
Software	Username	Password	Last Modified	Notes	Actions
Virtual Router Appliance (vRouter 5600)	vyatta	IzsKnsDS	6/17/2020	Click to edit	⋮
Virtual Router Appliance (vRouter 5600)	root	••••••••	6/17/2020	Click to edit	⋮

Open a browser and login to the Vyatta Gateway using:-

userID:- Vyatta
Password:- as show in the GUI

https://10.72.74.203

ssh vyatta@10.72.74.203

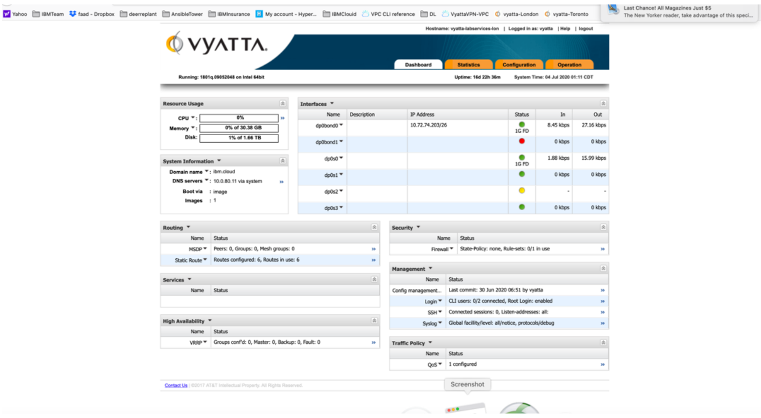


You have been logged out due to inactivity. Please login again:

Username: vyatta
Password: ••••••••

VYATTA
Help
LOGIN
Contact Us | ©2017 AT&T Intellectual Property. All Rights Reserved.
Screenshot

Login with the userID and password.



Hostname: vyatta-labservices-lon | Logged in as: vyatta | Help | logout

Running: 1801q.09052048 on Intel 64bit   Uptime: 16d 22h 36m   System Time: 04 Jul 2020 01:11 CDT

Resource Usage
CPU: 0%
Memory: 0% of 30.38 GB
Disk: 1% of 1.66 TB

System Information
Domain name: ibm.cloud
DNS servers: 10.0.80.11 via system
Boot via: image
Images: 1

Interfaces

Name	Description	IP Address	Status	In	Out
dp0bond0		10.72.74.203/26	🟢 1G FD	8.45 kbps	27.16 kbps
dp0bond1			🔴	0 kbps	0 kbps
dp0s0			🟢 1G FD	1.88 kbps	15.99 kbps
dp0s1			🟢	0 kbps	0 kbps
dp0s2			🟡	-	-
dp0s3			🟢	0 kbps	0 kbps

Routing

Name	Status
MSDP	Peers: 0, Groups: 0, Mesh groups: 0
Static Route	Routes configured: 6, Routes in use: 6

Services

Name	Status

High Availability

Name	Status
VRRP	Groups conf'd: 0, Master: 0, Backup: 0, Fault: 0

Security

Name	Status
Firewall	State-Policy: none, Rule-sets: 0/1 in use

Management

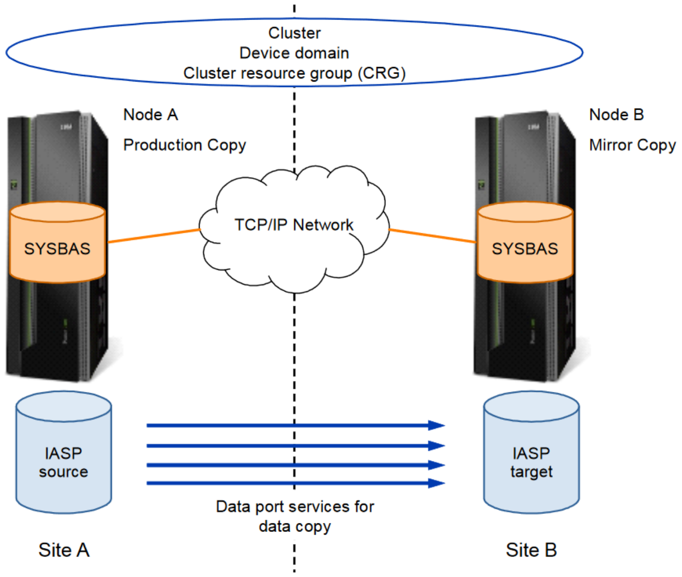
Name	Status
Config management...	Last commit: 30 Jun 2020 06:51 by vyatta
Login	CLI users: 0/2 connected, Root Login: enabled
SSH	Connected sessions: 0, Listen-addresses: all:
Syslog	Global facility/level: all/notice, protocols/debug

Traffic Policy

Name	Status
QoS	1 configured

VYATTA
Dashboard
Statistics
Configuration
Operation
Contact Us | ©2017 AT&T Intellectual Property. All Rights Reserved.
Screenshot

SOLUTION DIAGRAM:-



SOLUTION COMPONENTS AND REQUIREMENTS:-

COMPONENTS:-

This solution uses the following components:-

1. Open an IBM Cloud account

2. Create two Power PowerVS location Services and a private subnet in each PowerVS location.

3. Provision IBM i VSIs in each PowerVS location

a. A "production" IBM i cloud instance with an Independent ASP (IASP) that has been IASP-enabled (i.e. All changes/modifications allowing the IASP to function in a working environment should be completed before Geographic Mirroring is set up for a DR solution.)

b. A "DR" IBM i cloud instance with non-configured disks to be used for Geographic Mirroring. It is highly recommended that the number, type and capacity of disks match that of the production IASP.

4. Order Direct Link Connect Classic to connect each PowerVS location to IBM Cloud

5. Order two Vyatta Gateways one in each datacenter to allow for PowerVS location-to-location communication

6. Request a Generic Routing Encapsulation (GRE) tunnel to be provisioned at each PowerVS location.

7. Configure three GRE tunnels in the Vyatta Gateways. Two to connect Vyatta Gateway to the PowerVS location GRE tunnels created in Step 6 above and one across Vyatta Gateways to connect Vyatta-to-Vyatta. This will allow end-to-end PowerVS location-to-location communication for the VSIs in the PowerVS locations and to the IBM Cloud VSIs and other services such as Cloud Object Storage (COS) (if used).

8. Configure a Reverse-proxy Centos VSI to allow access to Private Cloud Object Storage endpoint from PowerVS location

PowerHA GEOGRAPHIC MIRRORING:-

When creating the IBM i instances via IBM Cloud Services, take note of the following recommendations in preparation for building the environments:-

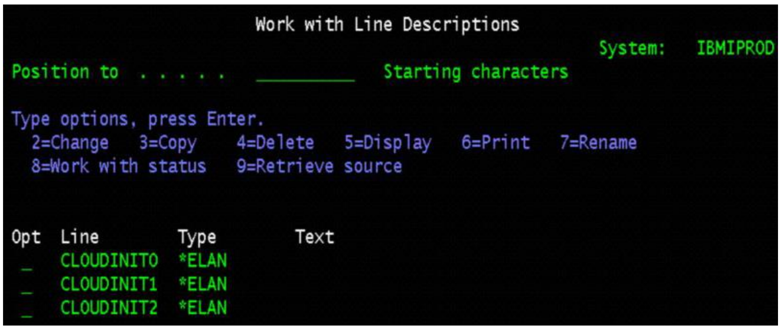
Production IBM i Creation:-

a. A general rule of thumb, assuming most production database objects are moved to the IASP, is a 1:3 ratio of SYSBAS volumes to IASP volumes. Much larger environments may see closer to a 1:6 or 1:9 ratio, as the size of SYSBAS does not need to grow at the same rate as the IASP.

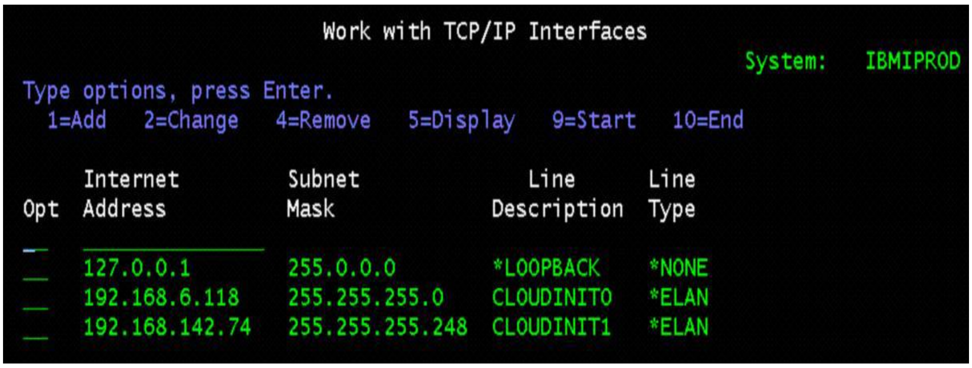
b. The names of the disks (from IBM Cloud Services) across ALL instances within that server must be unique. These names will not present themselves in the IBM i interface, but only be visible from the Cloud interface. This is why it is useful to keep track individually of the disk unit ID (from IBM i interface) and disk name (from Cloud interface) so you can assign your disks to the appropriate ASP. As noted above, these are best created at a later step in the process.

c. Once the instance is created and Active, open the console and wait for the log-in screen. If the default image was deployed, the qsecofr password (QSECOFR) will be disabled and need to be changed

d. Note that the line descriptions get created as CLOUDINITx names, and the TCP/IP interfaces are assigned to those automatically. The line descriptions are configured as **ONLINE(*YES)** and TCP/IP interfaces are configured as **AUTOSTART(*YES)** but can be changed to fit the needs of the business.



```
                         Work with Line Descriptions
                                                        System:   IBMIPROD
Position to  . . . . .   __________   Starting characters

Type options, press Enter.
  2=Change   3=Copy    4=Delete   5=Display   6=Print   7=Rename
  8=Work with status   9=Retrieve source


Opt  Line        Type        Text
 _   CLOUDINIT0  *ELAN
 _   CLOUDINIT1  *ELAN
 _   CLOUDINIT2  *ELAN
```



```
                         Work with TCP/IP Interfaces
                                                        System:   IBMIPROD
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet              Line        Line
Opt  Address          Mask                Description Type

__   _______________
__   127.0.0.1        255.0.0.0           *LOOPBACK   *NONE
__   192.168.6.118    255.255.255.0       CLOUDINIT0  *ELAN
__   192.168.142.74   255.255.255.248     CLOUDINIT1  *ELAN
```

Once TCP/IP is configured, the following changes are recommended:-

• CHGSYSVAL SYSVAL(QIPLTYPE) VALUE(1)

Note:- This will be changed back after DST/SST password is changed upon the next IPL.

• CHGSYSVAL SYSVAL(QLMTSECOFR) VALUE(0)

• **CHGSYSVAL SYSVAL(QAUTOVRT) VALUE(100)**

Note:- This can be any number desired, above zero.

• CHGTCPSVR SVRSPCVAL(*TELNET) AUTOSTART(*YES)

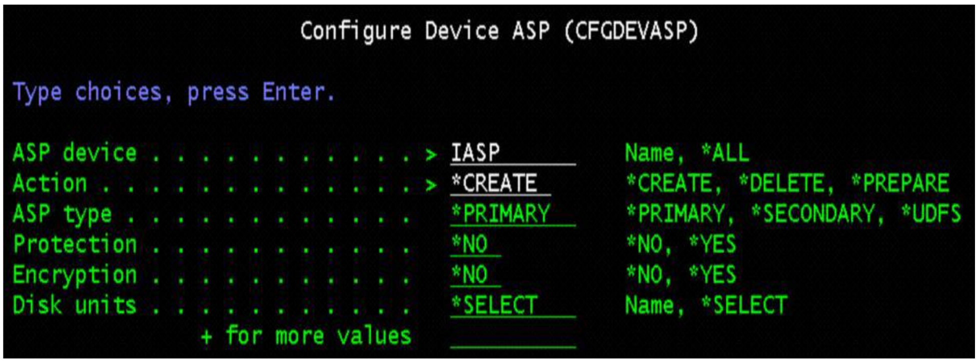
• CHGTCPSVR SVRSPCVAL(*FTP) AUTOSTART(*YES)

• CHGTCPSVR SVRSPCVAL(*SSHD) AUTOSTART(*YES)

• **CHGTCPSVR SVRSPCVAL(*INETD) AUTOSTART(*YES)**
IASP CREATION

To create the IASP, do the following:-

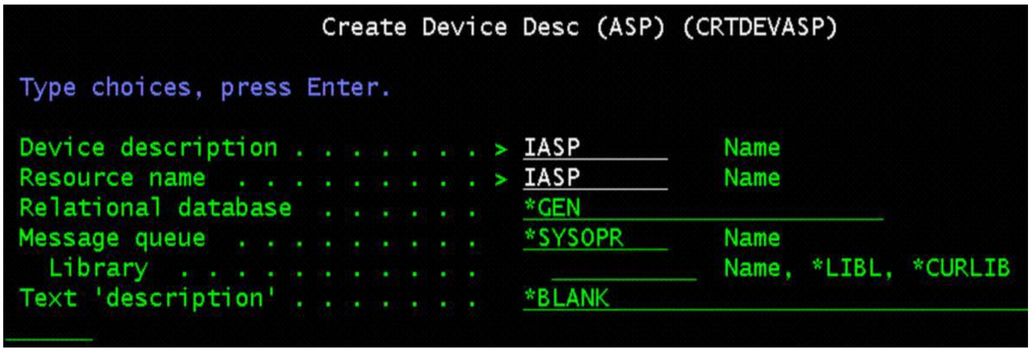
CFGDEVASP ASPDEV(<IASP Name>**) ACTION(*CREATE) TYPE(*PRIMARY) PROTECT(*NO) ENCRYPT(*NO) UNITS(*SELECT)**



```
                         Configure Device ASP (CFGDEVASP)

Type choices, press Enter.

ASP device . . . . . . . . . . . > IASP          Name, *ALL
Action . . . . . . . . . . . . . > *CREATE       *CREATE, *DELETE, *PREPARE
ASP type . . . . . . . . . . . .   *PRIMARY      *PRIMARY, *SECONDARY, *UDFS
Protection . . . . . . . . . . .   *NO           *NO, *YES
Encryption . . . . . . . . . . .   *NO           *NO, *YES
Disk units . . . . . . . . . . .   *SELECT       Name, *SELECT
               + for more values   __________
```

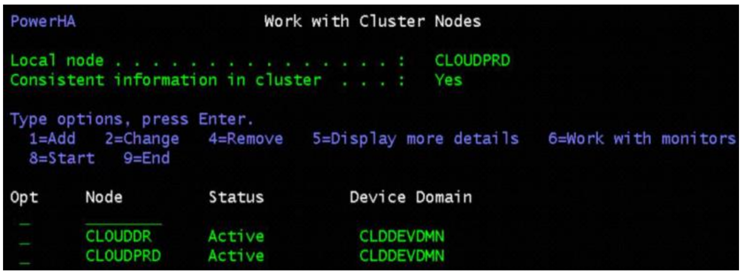
At any time, a matching device description can be created on the HA/DR node with the following:-

CRTDEVASP(<IASP Name>**) RSRCNAME(**<IASP Name>**)**



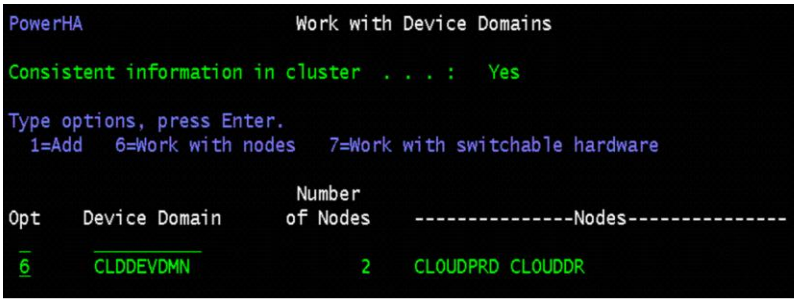
```
                         Create Device Desc (ASP) (CRTDEVASP)

Type choices, press Enter.

Device description . . . . . . . > IASP          Name
Resource name  . . . . . . . . . > IASP          Name
Relational database  . . . . . .   *GEN
Message queue  . . . . . . . . .   *SYSOPR       Name
  Library  . . . . . . . . . . .     __________  Name, *LIBL, *CURLIB
Text 'description' . . . . . . .   *BLANK
```

PowerHA Clustering Configuration:-

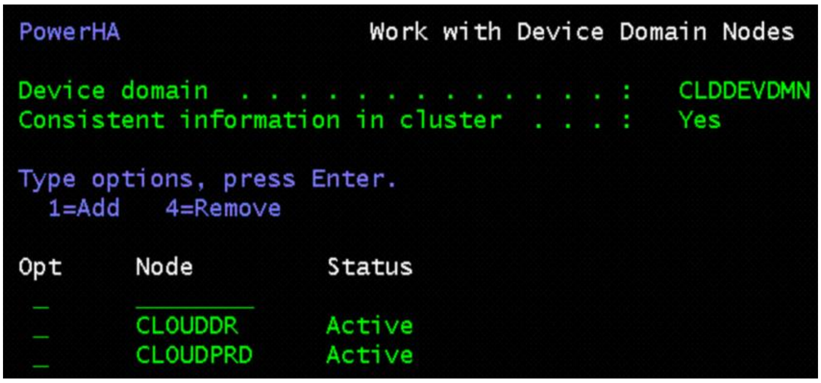


```
PowerHA                     Work with Cluster Nodes

Local node . . . . . . . . . . . . . . . :   CLOUDPRD
Consistent information in cluster  . . . :   Yes

Type options, press Enter.
  1=Add    2=Change    4=Remove    5=Display more details    6=Work with monitors
  8=Start    9=End

Opt     Node         Status          Device Domain

 _      CLOUDDR      Active           CLDDEVDMN
 _      CLOUDPRD     Active           CLDDEVDMN
```

Adding Cluster Nodes to Device Domain:-

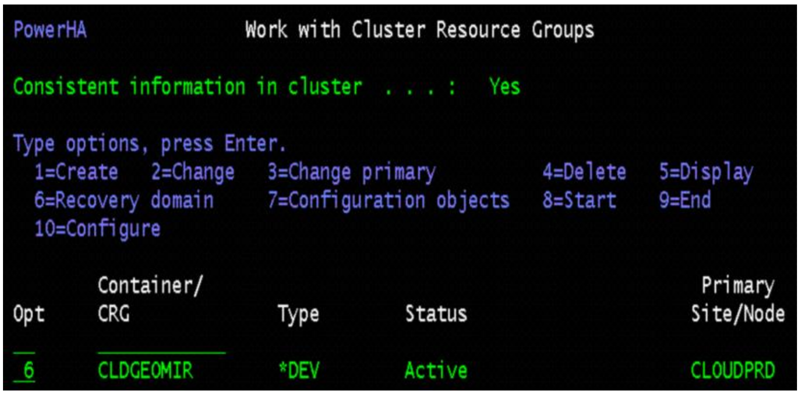


```
PowerHA                       Work with Device Domains

Consistent information in cluster  . . . :   Yes

Type options, press Enter.
  1=Add    6=Work with nodes    7=Work with switchable hardware

                               Number
Opt    Device Domain          of Nodes     --------------Nodes--------------
 _
 6      CLDDEVDMN                  2     CLOUDPRD CLOUDDR
```



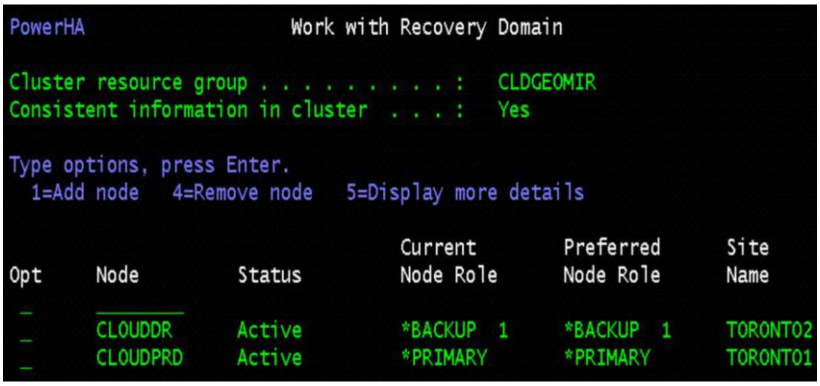
```
PowerHA                       Work with Device Domain Nodes

Device domain  . . . . . . . . . . . . . . :    CLDDEVDMN
Consistent information in cluster  . . . :    Yes

Type options, press Enter.
  1=Add    4=Remove

Opt      Node            Status

 _
 _       CLOUDDR         Active
 _       CLOUDPRD        Active
```

Creating the Device Cluster Resource Group (CRG):-



```
PowerHA                    Work with Cluster Resource Groups

Consistent information in cluster  . . . :   Yes

Type options, press Enter.
  1=Create   2=Change    3=Change primary          4=Delete    5=Display
  6=Recovery domain      7=Configuration objects   8=Start     9=End
  10=Configure

        Container/                                                  Primary
Opt     CRG                Type         Status                      Site/Node
 _
 6      CLDGEOMIR          *DEV         Active                      CLOUDPRD
```

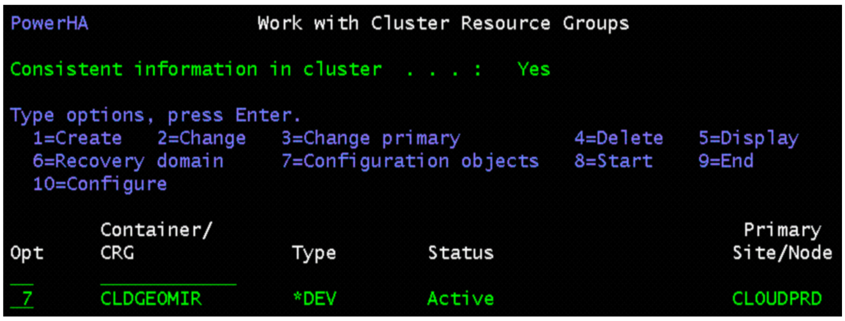
`



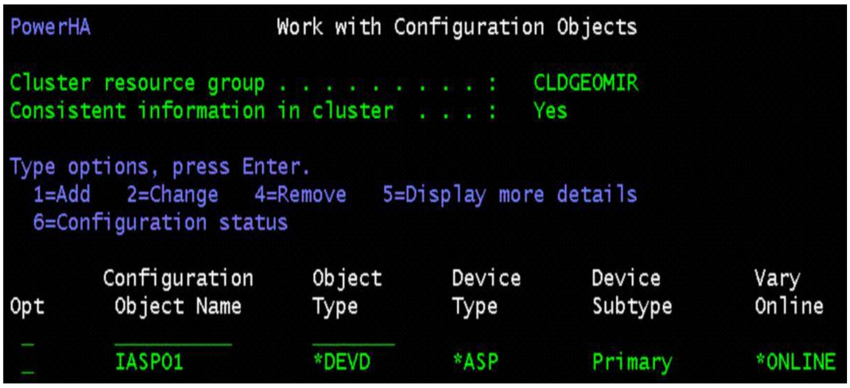
```
PowerHA                        Work with Recovery Domain

Cluster resource group . . . . . . . . . . :    CLDGEOMIR
Consistent information in cluster  . . . :    Yes

Type options, press Enter.
  1=Add node    4=Remove node    5=Display more details

                                        Current          Preferred         Site
Opt     Node           Status           Node Role        Node Role         Name
 _
 _      CLOUDDR        Active           *BACKUP   1      *BACKUP   1       TORONTO2
 _      CLOUDPRD       Active           *PRIMARY         *PRIMARY          TORONTO1
```

`

Add the IASP to the Device CRG:-



```
PowerHA                  Work with Cluster Resource Groups

Consistent information in cluster  . . . :   Yes

Type options, press Enter.
  1=Create    2=Change    3=Change primary          4=Delete    5=Display
  6=Recovery domain       7=Configuration objects   8=Start     9=End
  10=Configure

        Container/                                                     Primary
Opt     CRG              Type        Status                          Site/Node

 7      CLDGEOMIR        *DEV        Active                          CLOUDPRD
```



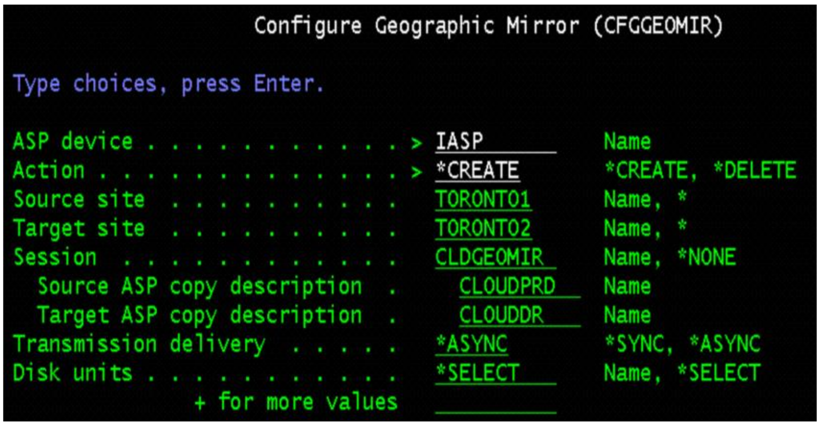
```
PowerHA                  Work with Configuration Objects

Cluster resource group . . . . . . . . . :   CLDGEOMIR
Consistent information in cluster  . . . :   Yes

Type options, press Enter.
  1=Add    2=Change    4=Remove    5=Display more details
  6=Configuration status

        Configuration     Object      Device      Device         Vary
Opt      Object Name      Type        Type        Subtype        Online

 _       IASP01           *DEVD       *ASP        Primary        *ONLINE
```

START GEOGRAPHIC MIRRORING OF THE IASP:-

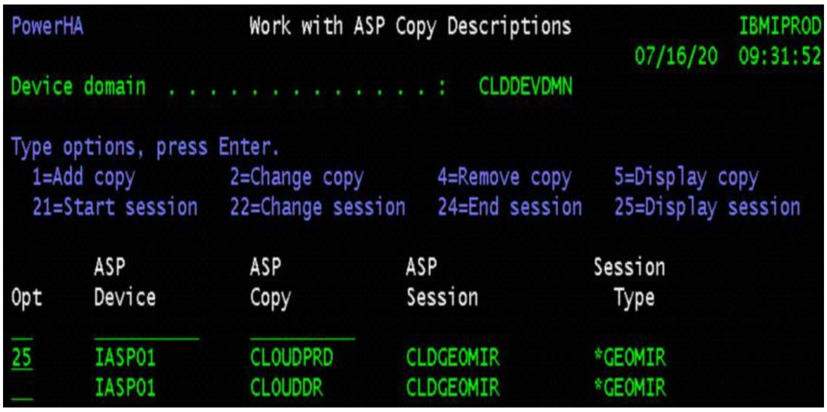
From the Production IBM i instance, do the following to start Geographic Mirroring on the IASP:-

1. **CFGGEOMIR ASPDEV(**<IASP Name>**) ACTION(*CREATE) SSN(**<DR Site ASP Copy>/<Prod Site ASP Copy>/<ASP
Session Name>**) DELIVERY(*ASYNC) UNITS(*SELECT)**.

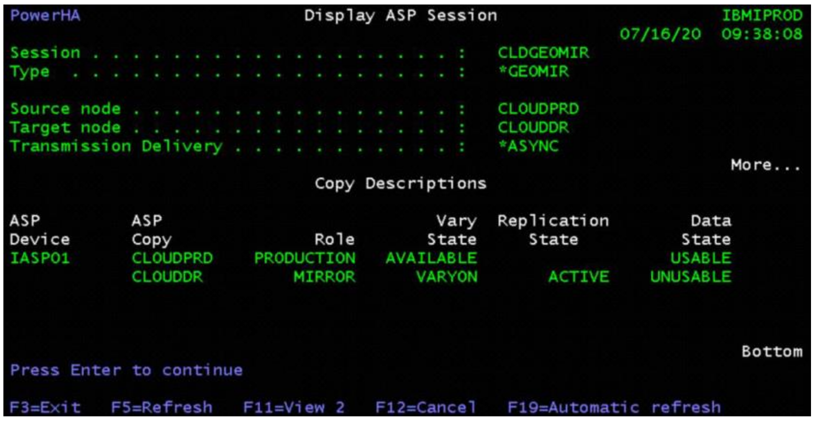
Press Enter.



```
                     Configure Geographic Mirror (CFGGEOMIR)

Type choices, press Enter.

ASP device . . . . . . . . . . . > IASP          Name
Action . . . . . . . . . . . . . > *CREATE       *CREATE, *DELETE
Source site  . . . . . . . . . .   TORONTO1      Name, *
Target site  . . . . . . . . . .   TORONTO2      Name, *
Session  . . . . . . . . . . . .   CLDGEOMIR     Name, *NONE
  Source ASP copy description  .     CLOUDPRD    Name
  Target ASP copy description  .     CLOUDDR     Name
Transmission delivery  . . . . .   *ASYNC        *SYNC, *ASYNC
Disk units . . . . . . . . . . .   *SELECT       Name, *SELECT
               + for more values
```



```
PowerHA              Work with ASP Copy Descriptions           IBMIPROD
                                                     07/16/20  09:31:52
Device domain . . . . . . . . . . . . . . :   CLDDEVDMN

Type options, press Enter.
  1=Add copy         2=Change copy       4=Remove copy    5=Display copy
  21=Start session   22=Change session   24=End session   25=Display session

        ASP            ASP            ASP               Session
Opt     Device         Copy           Session             Type

___     __________     __________
25      IASP01         CLOUDPRD       CLDGEOMIR         *GEOMIR
__      IASP01         CLOUDDR        CLDGEOMIR         *GEOMIR
```



```
PowerHA                     Display ASP Session                IBMIPROD
                                                      07/16/20  09:38:08
Session . . . . . . . . . . . . . . . . . . :   CLDGEOMIR
Type  . . . . . . . . . . . . . . . . . . . :   *GEOMIR

Source node . . . . . . . . . . . . . . . . :   CLOUDPRD
Target node . . . . . . . . . . . . . . . . :   CLOUDDR
Transmission Delivery . . . . . . . . . . . :   *ASYNC
                                                                More...
                            Copy Descriptions

ASP          ASP                           Vary  Replication        Data
Device       Copy               Role      State     State          State
IASP01       CLOUDPRD     PRODUCTION  AVAILABLE                   USABLE
             CLOUDDR          MIRROR     VARYON      ACTIVE     UNUSABLE



                                                                  Bottom
Press Enter to continue

F3=Exit   F5=Refresh   F11=View 2   F12=Cancel   F19=Automatic refresh
```

---------------- END OF THE DOCUMENT ----------------

Building Disaster Recovery Plan with IBM Cloud Virtual Servers

Definition:

A disaster recovery plan (DRP) is a documented plan that describes how an organization will recover from a disaster. A DRP should include steps to minimize the impact of a disaster on the organization's operations and to restore the organization to its normal state as quickly as possible.

A DRP is an essential part of any business continuity plan (BCP). A BCP is a comprehensive plan that outlines how an organization will maintain critical business functions during and after a disruption. The DRP is the part of the BCP that specifically addresses the recovery of IT systems and data.

A DRP should include the following information:

- A list of the organization's critical IT systems and data
- A risk assessment that identifies the most likely threats to the organization's IT systems and data
- A recovery strategy that outlines the steps that will be taken to restore the organization's IT systems and data in the event of a disaster
- A communication plan that outlines how the organization will communicate with employees, customers, and other stakeholders during and after a disaster
- A testing plan that outlines how the DRP will be tested on a regular basis

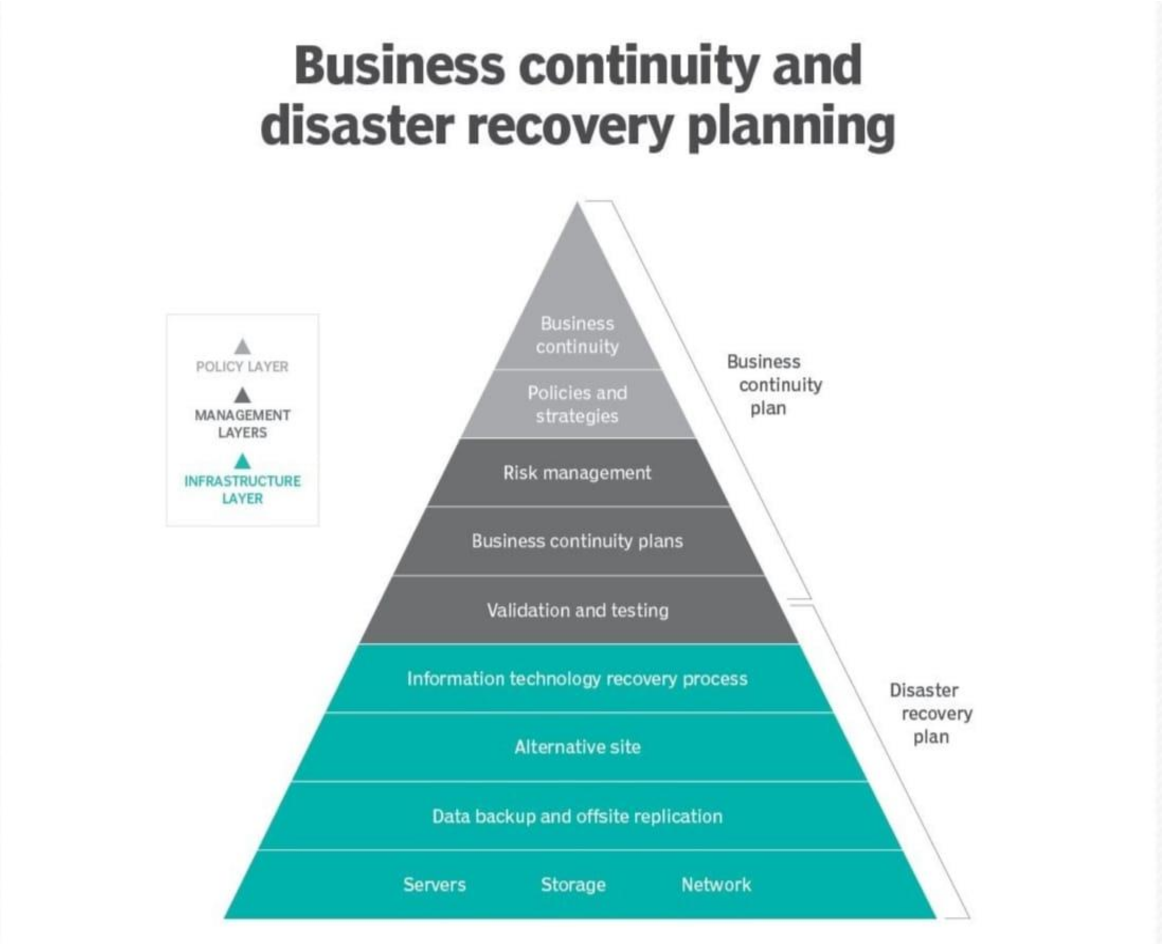
DRPs can be tailored to the specific needs of any organization. The size and complexity of the DRP will vary depending on the size and complexity of the organization's IT environment.

Here are some examples of disasters that a DRP should cover:

- Cyberattacks
- Hardware failures
- Power outages

- Software failures

By having a DRP in place, organizations can minimize the impact of disasters on their operations and get back to business as quickly as possible.



To build a disaster recovery plan with IBM Cloud Virtual Server, we will need to:

1.Assess your risks:

What are the most likely threats to your IBM Cloud Virtual Server environment? Natural disasters? Cyberattacks? Hardware failures? Once you have identified your risks, you can start to develop a plan to mitigate them.

2.Choose a disaster recovery solution:

IBM Cloud offers a variety of disaster recovery solutions, including:

- IBM Cloud Resiliency Services
- IBM Cloud Backup as a Service (BaaS)

- IBM Spectrum Protect Plus

IBM Cloud Resiliency Services:

A fully managed disaster recovery service that provides a comprehensive solution for protecting the data and applications.

IBM Cloud Backup as a Service (BaaS):

A cloud-based backup and recovery solution that allows to back up the data to IBM Cloud and restore it quickly and easily.

IBM Spectrum Protect Plus:

A software solution that provides comprehensive data protection for virtual machines, databases, and containers.

Design the disaster recovery plan:

This should include the following:

- Recovery point objective (RPO)
- Recovery time objective (RTO)
- Recovery procedures

Recovery point objective (RPO):

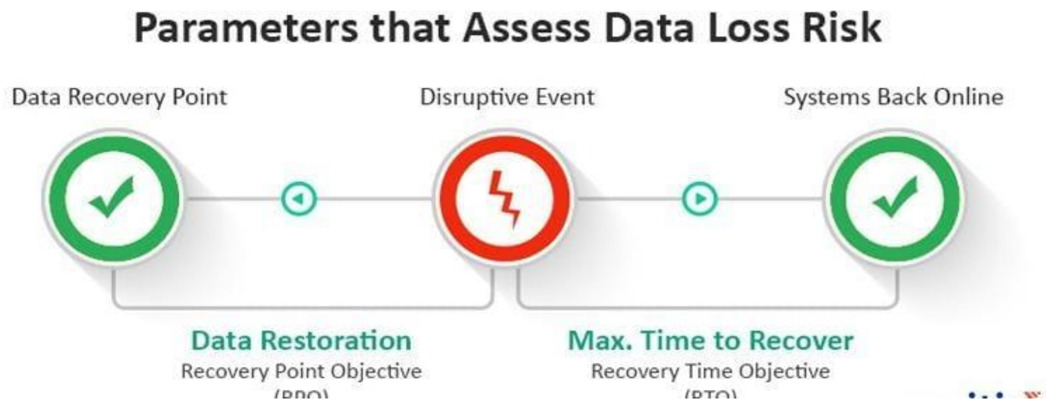
The maximum amount of data that can afford to lose in a disaster.

Recovery time objective (RTO):

The maximum amount of time that the systems can be down in a disaster.

Recovery procedures:

Step-by-step instructions for restoring the data and systems in a disaster.



4.Implement disaster recovery plan:

This includes setting up your chosen disaster recovery solution and configuring it to meet your RPO and RTO requirements.

5.Test disaster recovery plan:

It is important to regularly test your disaster recovery plan to ensure that it works as expected.

Here are some additional tips for building a disaster recovery plan with IBM Cloud Virtual Server

- **Use multiple regions:**

IBM Cloud has data centers in multiple regions around the world. This allows you to replicate the data and applications to a different region in the event of a disaster in primary region.

- **Use snapshots**:

Snapshots are point-in-time copies of virtual servers. You can use snapshots to quickly create backups of our virtual servers or to restore virtual servers to a previous state.

- **Use automation:**

IBM Cloud offers a variety of automation tools that can help, to automate the disaster recovery process. This can help to reduce the time and effort required to recover from a disaster.

Once we implemented our disaster recovery plan, it is important to regularly review and update it to ensure that it is still meeting our needs.

Conclusion:

IBM Cloud Virtual Server offers a variety of features and services that can help to build and implement a comprehensive disaster recovery plan. By following the steps outlined above, can create a disaster recovery plan that will help to protect our data and applications and minimize downtime in the event of a disaster.

IBM Cloud Virtual Server can help you to keep the business running even in the face of a disaster.

Team members:

1.VIGNESH .M

2.DARWIN KUMAR .R

3.SOUMYA SHIBU

4.VAISHALI.R

Building the Disaster Recovery Plan by configuring replication and testing recovery procedures.

Abstract:

Disaster recovery planning is essential for any business that relies on IT systems. By configuring replication and testing recovery procedures, businesses can ensure that they can quickly recover from a disaster and minimize disruption to their operations.

IBM Cloud virtual servers offer a number of features that make them ideal for disaster recovery planning, such as high availability, scalability, and security.

Step-by-step process for building a disaster recovery plan:

- Identify the critical virtual servers and data.
- Choose a replication solution:

  IBM Cloud offers a variety of replication solutions for virtual servers, including volume replication, instance replication, and live migration. Choose the solution that best meets our needs.
- Configure replication:

  The specific steps involved in configuring replication will vary depending on the solution that we choose. However, there are some general steps that are common to all replication solutions, such as creating a replication relationship between the source and target environments, selecting the virtual servers or data that you want to replicate, and configuring the replication schedule and other settings.

- Test the recovery procedures.

  Once we have configured replication, we need to test recovery procedures to make sure that they work. This involves simulating a disaster and then trying to recover the virtual servers from the replicated copy.
- Document the disaster recovery plan:

  The disaster recovery plan should include information such as a list of the critical virtual servers and data that are protected by the plan, a description of the replication solution that is used, and instructions on how to fail over to the test environment, fail back to the production environment, and restore the critical virtual servers and data from the replicated copy.
- Maintain and review the disaster recovery plan:

  The disaster recovery plan is a living document that should be maintained and reviewed on a regular basis to ensure that it is up-to-date and reflects the current state of IT environment.

By following these steps, can build a comprehensive disaster recovery plan that will help to protect the critical virtual servers and data from disaster and minimize disruption to business operations.

Brief explanation of the above steps

Step 1: Identify your critical virtual servers and data

The first step in building a disaster recovery plan is to identify the virtual servers and data that are essential to the business operations. These are the virtual servers and data that will need to protect with the disaster recovery plan.

To identify the critical virtual servers and data, can consider the following factors:

Impact on business operations:

How much would our business be impacted if a particular virtual server or data set were unavailable?

Compliance requirements:

Are there any compliance requirements that require to protect certain types of data?

Recovery time objective (RTO):

How quickly we need to be able to recover the virtual servers and data in the event of a disaster?

Recovery point objective (RPO):

How much data are we willing to lose in the event of a disaster?

Once you have identified your critical virtual servers and data, we can begin to develop

Step 2: Choose a replication solution

IBM Cloud offers a variety of replication solutions for virtual servers, including:

Volume replication:

Replicate volumes between two different IBM Cloud regions.

Instance replication:

Replicate entire virtual machine instances between two different IBM Cloud regions.

Live migration:

Live migrate virtual machine instances between two different IBM Cloud regions.

Choose the replication solution that best meets our needs.

Step 3: Configure replication

The specific steps involved in configuring replication will vary depending on the replication solution that we choose. However, there are some general steps that are common to all replication solutions:

- Create a replication relationship between the source and target environments.
- Select the virtual servers or data that we want to replicate.
- Configure the replication schedule and other settings.
- Start the replication process.

Example:

To configure volume replication between two different IBM Cloud regions using the IBM Cloud console:

1. Go to the Volumes page.
2. Select the volume that we want to replicate.
3. Click Actions > Replicate.
4. Select the target region and volume where we want to replicate the volume.
5. Click Replicate.

The replication process will begin immediately. Once the replication process is complete, we will have a copy of the source volume in the target region.

Step 4: Test the recovery procedures

Once we have configured replication, need to test our recovery procedures to make sure that they work. This involves simulating a disaster and then trying to recover our virtual servers from the replicated copy.

To test the recovery procedures:

- Create a test environment in the target region.
- Fail over to the test environment by stopping the virtual servers in the production environment and then starting the virtual servers in the test environment.
- Restore the most recent data from the replicated copy.
- Verify that the virtual servers in the test environment are working properly.
- Fail back to the production environment by stopping the virtual servers in the test environment and then starting the virtual servers in the production environment.

Step 5: Document the disaster recovery plan

Once we have tested our recovery procedures and documented the disaster recovery plan, we will have a comprehensive plan in place to protect our critical virtual servers and data from disaster.

The disaster recovery plan should include the following information:

- A list of the critical virtual servers and data that are protected by the disaster recovery plan.
- A description of the replication solution that is used to protect the critical virtual servers and data.
- Instructions on how to fail over to the test environment and how to fail back to the production environment.
- Instructions on how to restore the critical virtual servers and data from the replicated copy.

Step 6: Maintain and review the disaster recovery plan

The disaster recovery plan is a living document that should be maintained and reviewed on a regular basis. This will ensure that the plan is up-to-date and that it reflects the current state of the IT environment.

We should review our disaster recovery plan at least once per year, or more often if there are any significant changes to the IT environment.

Additional tips:

- When choosing a replication solution, consider your RTO and RPO requirements.
- Make sure to test our recovery procedures regularly to ensure that they work as expected.
- Document our disaster recovery plan and make it available to all relevant stakeholders.

Conclusion:

Building a disaster recovery plan is essential for any business that relies on IT systems. By configuring replication and testing recovery procedures using IBM Cloud virtual servers, businesses can ensure that they can quickly recover from a disaster and minimize disruption to their operations.

In short, IBM Cloud virtual servers provide a reliable and scalable platform for building a comprehensive disaster recovery plan. By following the steps outlined in this article, businesses can protect their critical data and applications, minimize disruption to their operations, and ensure that their business is prepared to handle any disaster.