Phase 4
DISASTER RECOVERY

Name:R.Ramyasri

Dept: Computer science and engineering

Year:III Yr

College: University College of Engineering Thirukkuvalai

Disaster recovery

Disaster recovery is the practice of anticipating, planning for, surviving, and recovering from a disaster that may affect a business. Disasters can include:

Natural events like earthquakes or hurricanes

Failure of equipment or infrastructure, such as a power outage or hard disk failure

Man-made calamities such as accidental erasure of data or loss of equipment

Cyber attacks by hackers or malicious insiders

Disaster recovery plan

A disaster recovery plan enables businesses to respond quickly to a disaster and take immediate action to reduce damage, and resume operations as quickly as possible.

A disaster recovery plan typically includes:

Emergency procedures staff can carry out when a disaster occurs

Critical IT assets and their maximum allowed outage time

Tools or technologies that should be used for recovery

A disaster recovery team, their contact information and communication procedures (e.g. who should be notified in case of disaster)

Building Your Disaster Recovery Plan

- Here are key steps to help guide you through the process of creating a disaster recovery plan:
-
- Risk Assessment
- A disaster recovery plan should start with business impact analysis (BIA) and risk assessment that address the relevant potential disasters. Here are key aspects of considerations:
-
- Analyze all functional areas of the organization – this analysis can help you identify possible consequences, such as data loss or leakage.
- Evaluate risks and define suitable goals – disaster recovery is a key component in larger business continuity plans. Evaluating risks and setting goals can help organizations recover critical business operations that enable continuity even while IT teams address the incident.
- Determine geographical and infrastructure risk factors – a risk analysis should factor these complex risks to enable organizations to prepare a suitable recovery strategy for these events. You should determine whether you need cloud backup, whether a single site will suffice or do you need multiple sites, and who is allowed access.

- Evaluate Critical Needs
- Once you have completed a risk assessment, you need to evaluate the critical needs of each department and establish priorities for operations and processing. It involves creating written agreements for predetermined alternatives and specifying the following details:
-
- Special security procedures
- Availability, cost, and duration
- Guarantee of compatibility
- Hours of operation
- Scenarios the organization defines as emergencies
- System testing
- A procedure for notifying users of system changes
- Personnel requirements
- Specifications of hardware required for critical processes
- Service extension negotiation process
- Any relevant contractual issue

Set Disaster Recovery Plan Objectives

- Create a list of mission-critical operations needed for business continuity – when creating your list, decide which applications, data, user accesses, and equipment are needed to support these operations.
- Document your RTO and RPO – finalize the required RTO and RPO for each critical asset and document it.
- Assess service level agreements (SLAs) – all of your objectives should account for SLAs promised to any stakeholder, including users and executives.

Collect Data and Create the Written Document

- Lists – include critical contact information lists, master vendor lists, backup employee position listings, notification checklists, master call lists.
- Inventories – include communications equipment, documentation, data center computer hardware, forms, microcomputer hardware and software, insurance policies, office equipment, workgroup hardware, and off-site storage location equipment.

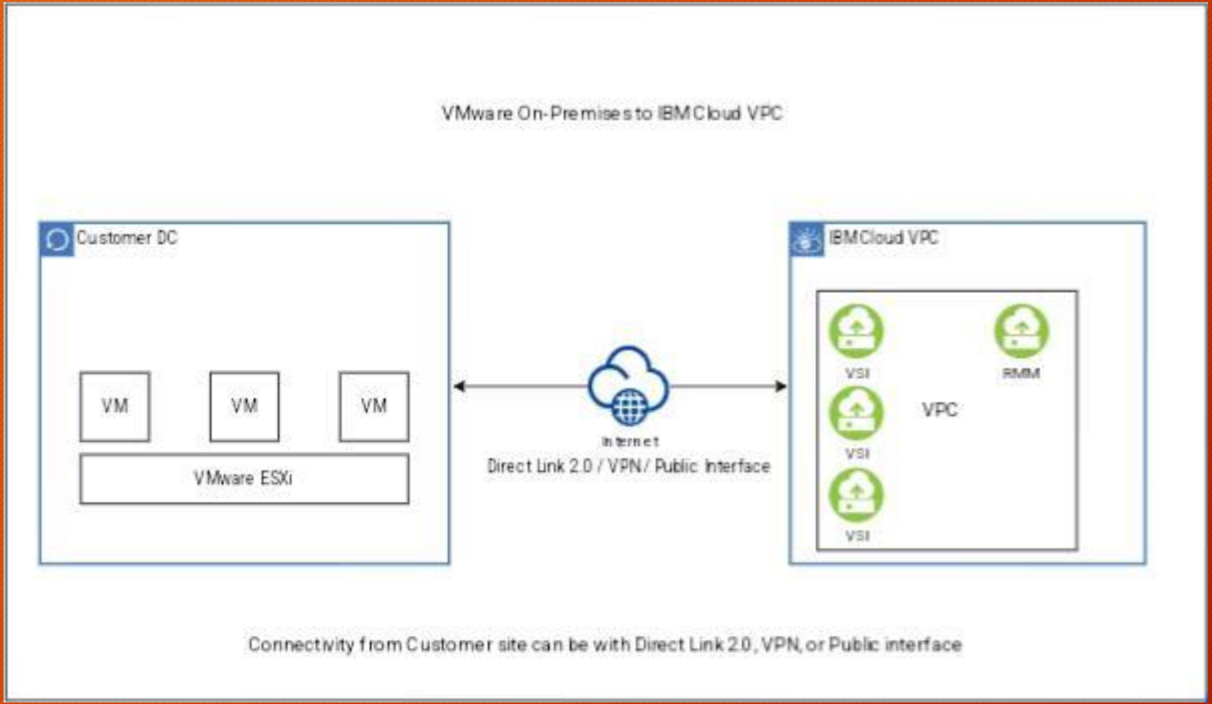
- Schedules – include schedules defined for software and data files backup or retention.
- Procedures – include all procedures defined for system restore or recovery.
- Locations – include all temporary disaster recovery locations.
- Documentation – include any relevant inventories, materials, and lists.
- Organize and include this data in a written, documented plan.

On-premises Vmware VM to IBM Cloud VPC migration with RMM

- To implement a data center transformation, the RackWare Management Module (RMM) migration solution provides a seamless virtual-to-virtual replatforming for Vmware virtual machine (VM) to IBM Cloud® virtual server instance migration. It allows the adoption of existing capabilities of IBM Cloud. Its intuitive GUI allows you to move the OS, application, and data from Vmware ESXi to IBM Cloud VPC virtual server instance.
-
- This guide shows you how to complete a migration from your on-premises Vmware VM to IBM Cloud VPC.

- CentOS 7.8, 7.9
- RHEL 7.2, 7.3, 7.4, 8.1
- Ubuntu 18.04, 20.04
- Debian 9.x, 10.x
- Windows 2012, 2012R2, 2016, 2019

Architecture diagram



VMware On-Premises to IBM Cloud VPC

Connectivity from Customer site can be with Direct Link 2.0, VPN, or Public interface

Step 1:Order RMM

- The RMM tool is available in the IBM Cloud catalog. After you order, a virtual server with RMM software is installed into your VPC of choice. The RMM server has a public IP address for reachability and a default login.
- Order the RMM server from the IBM Cloud catalog.
- After you order, log in to the RMM server.
- In the RMM server, change the default password, create users, and create an SSH key.
- Upload the SSH key to IBM Cloud VPC.

Step 2:Bring your own licence from Rack ware

Generate a license file in /etc/rackware by running the following command:

```
vadm relicense
```

You need to purchase the license from RackWare by emailing the generated license file to ensing@rackwareinc.com or sales@rackwareinc.com.

After you receive a valid license, download the license file and place it in /etc/rackware. Restart e services to apply the license by running the following command:

```
adm restart
```

ou need to purchase the license from RackWare by emailing the generated license file to ensing@rackwareinc.com or sales@rackwareinc.com.

ter you receive a valid license, download the license file and place it in /etc/rackware. Restart the rvices to apply the license by running the following command:

Step 3: connectivity Options between The customer Data center and IBM Cloud VPC

Your source and target server should communicate with each other and the RMM. This can be done over the public internet with public Ips or with a private-only environment. If you have a private-only environment, you must set up either a VPN or

Step 4:Set up and provision VPC and virtual server instances

- Option 1: manual
- The RMM solution handles the OS, application, and data movement. It does not need to set up a VPC target side; you need to handle the setup. You first set up the VPC infrastructure. At a bare minimum, you must set up a VPC, subnets, and the corresponding virtual server instances that you are planning to migrate. The new target virtual server instance profile (vCPU and vMemory) does not need to match the source. However, as for the storage, it needs to be the same or greater in size.

- “Create a VPC.
- Create subnets.
- Order the virtual server instance.
- SSH key (RMM SSH keys need to be added in addition to bastion SSH key)
- Operating system name (Linux or Windows and their respective version)
- Security groups
- Secondary volume”

Option 2:auto provision

- RMM can automatically provision a virtual server instance of VPC. Enable the wave level setting Autoprovision and then configure RMM with necessary details. Use these steps to use the auto-provision feature:
-
- Setting up a cloud user
-
- Log in to the RackWare web console.
- In the RackWare web console, navigate to Configuration > Clouduser.
- When you add a cloud user, enter a name and select IBM Cloud VPC for the Cloud Provider. Select the region where you want to auto-provision the virtual server instance, and enter your IBM Cloud API key.
- Click Add.

Conduct recovery tests to ensure that the disaster recovery plan works as intended

- One of the main goals of a disaster recovery test is to determine if a DR plan can work and meet an organization’s predetermined RPO/RTO requirements. It also provides feedback to enterprises so they can amend their DR plan should any unexpected issues arise.

What is a disaster recovery plan?

- It is most effective to develop an information technology (IT) disaster recovery plan in conjunction with the business continuity plan (BCP). A business continuity plan is a complete organizational plan that consists of five components:
-
- 1. Business resumption plan
- 2. Occupant emergency plan
- 3. Continuity of operations plan
- 4. Incident management plan (IMP)
- 5. Disaster recovery plan

- Every situation is unique and there is no single correct way to develop a disaster recovery plan. However, there are three principal goals of disaster recovery that form the core of most DRPs:
-
- prevention, including proper backups, generators, and surge protectors
- detection of new potential threats, a natural byproduct of routine inspections
- correction, which might include holding a “lessons learned” brainstorming session and securing proper insurance policies

Disaster recovery plan

- Personnel
- Every disaster recovery plan must detail the personnel who are responsible for the execution of the DR plan, and make provisions for individual people becoming unavailable.
-
- IT inventory
- An updated IT inventory must list the details about all hardware and software assets, as well as any cloud services necessary for the company's operation, including whether or not they are business critical, and whether they are owned, leased, or used as a service

- Backup procedures
- The DRP must set forth how each data resource is backed up – exactly where, on which devices and in which folders, and how the team should recover each resource from backup.
-
- Disaster recovery procedures
- These specific procedures, distinct from backup procedures, should detail all emergency responses, including last-minute backups, mitigation procedures, limitation of damages, and eradication of cybersecurity threats.

- Disaster recovery sites
- Any robust disaster recovery plan should designate a hot disaster recovery site. Located remotely, all data can be frequently backed up to or replicated at a hot disaster recovery site — an alternative data center holding all critical systems. This way, when disaster strikes, operations can be instantly switched over to the hot site.

- Restoration procedures
- Finally, follow best practices to ensure a disaster recovery plan includes detailed restoration procedures for recovering from a loss of full systems operations. In other words, every detail to get each aspect of the business back online should be in the plan, even if you start with a disaster recovery plan template. Here are some procedures to consider at each step.
-
- Include not just objectives such as the results of risk analysis and RPOs, RTOs, and SLAs, but also a structured approach for meeting these goals. The DRP must address each type of downtime and disaster with a step-by-step plan, including data loss, flooding, natural disasters, power outages, ransomware, server failure, site-wide outages, and other issues. Be sure to enrich any IT disaster recovery plan template with these critical details.

Benefits of a disaster recovery plan

- Cost-efficiency
- Disaster recovery plans include various components that improve cost-efficiency. The most important elements include prevention, detection, and correction, as discussed above. Preventative measures reduce the risks from man-made disasters. Detection measures are designed to quickly identify problems when they do happen, and corrective measures restore lost data and enable a rapid resumption of operations.
- Increased productivity
- Designating specific roles and responsibilities along with accountability as a disaster recovery plan demands increases effectiveness and productivity in your team. It also ensures redundancies in personnel for key tasks, improving sick day productivity, and reducing the costs of turnover.

- Scalability
- Planning disaster recovery allows businesses to identify innovative solutions to reduce the costs of archive maintenance, backups, and recovery. Cloud-based data storage and related technologies enhance and simplify the process and add flexibility and scalability.
-
- The disaster recovery planning process can reduce the risk of human error, eliminate superfluous hardware, and streamline the entire IT process. In this way, the planning process itself becomes one of the advantages of disaster recovery planning, streamlining the business, and rendering it more profitable and resilient before anything ever goes wrong.

- Improved customer retention
- Customers do not easily forgive failures or downtime, especially if they result in loss of sensitive data. Disaster recovery planning helps organizations meet and maintain a higher quality of service in every situation. Reducing the risks your customers face from data loss and downtime ensures they receive better service from you during and after a disaster, shoring up their loyalty.
-
- Compliance
- Enterprise business users, financial markets, healthcare patients, and government entities, all rely on availability, uptime, and the disaster recovery plans of important organizations. These organizations in turn rely on their DRPs to stay compliant with industry regulations such as HIPAA and FINRA.

Ways to develop a disaster recovery plan

- Risk assessment
- First, perform a risk assessment and business impact analysis (BIA) that addresses many potential disasters. Analyze each functional area of the organization to determine possible consequences from middle of the road scenarios to “worst-case” situations, such as total loss of the main building. Robust disaster recovery plans set goals by evaluating risks up front, as part of the larger business continuity plan, to allow critical business operations to continue for customers and users as IT addresses the event and its fallout.

- Evaluate critical needs
- Next, establish priorities for operations and processing by evaluating the critical needs of each department. Prepare written agreements for selected alternatives, and include details specifying all special security procedures, availability, cost, duration, guarantee of compatibility, hours of operation, what constitutes an emergency, non-mainframe resource requirements, system testing, termination conditions, a procedure notifying users of system changes, personnel requirements, specs on required processing hardware and other equipment, a service extension negotiation process, and other contractual issues.

- Set disaster recovery plan objectives
- Create a list of mission-critical operations to plan for business continuity, and then determine which data, applications, equipment, or user accesses are necessary to support those functions. Based on the cost of downtime, determine each function’s recovery time objective (RTO). This is the target amount of time in hours, minutes, or seconds an operation or application can be offline without an unacceptable business impact.
-
- Determine the recovery point objective (RPO), or the point in time back to which you must recover the application. This is essentially the amount of data the organization can afford to lose.
-
- Assess any service level agreements (SLAs) that your organization has promised to users, executives, or other stakeholders.

- Collect data and create the written document
- Collect data for your plan using pre-formatted forms as needed. Data to collect in this stage may include:
-
- lists (critical contact information list, backup employee position listing, master vendor list, master call list, notification checklist)
- inventories (communications equipment, data center computer hardware, documentation, forms, insurance policies, microcomputer hardware and software, office equipment, off-site storage location equipment, workgroup hardware, etc.)
- schedules for software and data files backup/retention
- procedures for system restore/recovery
- temporary disaster recovery locations
- other documentation, inventories, lists, and materials