Name:B.Srila

Register no:822221104038

Dept: Computer science and engineering

Year:III

Title:IBM Disaster Recovery

College:University college of engineering –Thirukkuvalai

What is Disaster Recovery?

- ***Disaster Recovery (DR)Consists of IT technologies and best practices designed to prevent or minimize data loss and business disruption resulting from catastrophic events everything from equipment failures and localized power outages to cyberattacks, civil emergencies, criminal or military attacks, and natural disasters.***

Bussiness Continuity Planning

- Bussiness Continuity Planning creates systems and processes to ensure that all areas of your enterprise will be able to maintain essential operations or be able to resume them as quickly as possible in the event of a crisis or emergency.
- Disaster recovery planning is the subset of business continuity planning that focuses on recovering IT infrastructure and systems.

Disaster recovery planning (Business impact analysis)

- The creation of a comprehensive disaster recovery plan begins with business impact analysis. When performing this analysis, you'll create a series of detailed disaster scenarios that can then be used to predict the size and scope of the losses you'd incur if certain business processes were disrupted .
- This will allow you to identify the areas and functions of the business that are the most critical and enable you to determine how much downtime each of these critical functions could tolerate. With this information in hand, you can begin to create a plan for how the most critical operations could be maintained in various scenarios.

Risk analysis

- Assessing the likelihood and potential consequences of the risks your business faces is also an essential component of disaster recovery planning.
- As cyberattacks and ransomware become more prevalent, it's critical to understand the general cybersecurity risks that all enterprises confront today as well as the risks that are specific to your industry and geographical location.

Prioritizing applications

- Not all workloads are equally critical to your business's ability to maintain operations, and downtime is far more tolerable for some applications than it is for others. Separate your systems and applications into three tiers, depending on how long you could stand to have them be down and how serious the consequences of data loss would be.

- 1.Mission-critical: Applications whose functioning is essential to your business's survival.
- 2.Important: Applications for which you could tolerate relatively short periods of downtime.
- 3.Non-essential: Applications you could temporarily replace with manual processes or do without.

Establishing recovery time objectives, recovery point objectives.

- By Considering your risk and business impact analyses, you should be able to establish objectives for how long you'd need it to take to bring systems back up, how much data you could stand to use, and how much data corruption or deviation you could tolerate.
- Your recovery time objective (RTO) is the maximum amount of time it should take to restore application or system functioning following a service disruption.
- Your recovery point objective (RPO) is the maximum age of the data that must be recovered in order for your business to resume regular operations. For some businesses, losing even a few minutes' worth of data can be catastrophic, while those in other industries may be able to tolerate longer windows.

Recovery Consistency Objectives.

- A recovery consistency objective (RCO) is established in the service-level agreement (SLA) for continuous data protection services.
- It is a metric that indicates how many inconsistent entries in business data from recovered processes or systems are tolerable in disaster recovery situations, describing business data integrity across complex application environments.

Regulatory compliance issues

- All disaster recovery software and solutions that your enterprise have established must satisfy any data protection and security requirements that you're mandated to adhere to. This means that all data backup and failover systems must be designed to meet the same standards for ensuring data confidentiality and integrity as your primary systems.
- At the same time, several regulatory standards stipulate that all businesses must maintain disaster recovery and/or business continuity plans. The Sarbanes-Oxley Act (SOX), for instance, requires all publicly held firms in the U.S. To maintain copies of all business records for a minimum of five years. Failure to comply with this regulation (including neglecting to establish and test appropriate data backup systems) can result in significant financial penalties for companies and even jail time for their leaders.

Choosing recovery site locations

- Building your own disaster recovery data center involves balancing several competing objectives. On the one hand, a copy of your data should be stored somewhere that's geographically distant enough from your headquarters or office locations that it won't be affected by the same seismic events, environmental threats, or other hazards as your main site.
- On the other hand, backups stored offsite always take longer to restore from than those located on-premises at the primary site, and network latency can be even greater across longer distances.

Continuous testing and review

- Simply put, if your disaster recovery plan has not been tested, it cannot be relied upon. All employees with relevant responsibilities should participate in the disaster recovery test exercise, which may include maintaining operations from the failover site for a period of time.
- The IBM Knowledge Center provides an example of a disaster recovery plan.

Disaster Recovery-as-a-Service (DRaaS)

- **Disaster recovery service offerings differ from vendor to vendor. Some vendors define their offering as a comprehensive, all-in-one solution, while others offer piecemeal services ranging from single application restoration to full data center replication in the cloud.**
- **Some offerings may include disaster recovery planning or testing services, while others will charge an additional consulting fee for these offerings.**