Disaster Recovery with IBM Cloud Virtual Servers

Phase 3: Development Part 1

IBM Cloud Disaster Recovery

Creating a disaster recovery plan using IBM Cloud Virtual Servers involves several key steps. Here's an overview of the process:

Assessment and Planning:

Identify critical virtual machines (VMs) and their specific roles in your infrastructure.

Determine your Recovery Time Objective (RTO), i.e., how quickly you need to recover after a disaster.

Define your Recovery Point Objective (RPO), which establishes how much data loss is acceptable.

Prioritize VMs based on their importance to your business operations.

Selecting IBM Cloud Services:

Choose appropriate IBM Cloud Virtual Server configurations to host your VMs.

Consider IBM Cloud services like Block Storage, Object Storage, and Load Balancers for redundancy and data integrity.

Setting up Regular Backups:

Use IBM Cloud's backup and snapshot features for regular backups.

Configure backup schedules and retention policies based on your RPO requirements.

Testing and Validation:

Regularly test your disaster recovery plan to ensure it meets your RTO and RPO goals.

Conduct failover and failback tests to confirm the effectiveness of your strategy.

Documentation:

Maintain detailed documentation of your disaster recovery plan, including configurations, contact information, and procedures.

Automation and Scripts:

Develop automation scripts for VM deployment, configuration, and failover to reduce recovery time.

Implement monitoring and alerting systems to detect potential issues.

Security and Access Controls:

Implement security measures to protect your VMs and data, including firewalls and access controls.

Communication Plan:

Define a communication plan for informing stakeholders and employees during a disaster event.

Review and Updates:

Regularly review and update your disaster recovery plan to account for changes in your infrastructure and business requirements.

Remember that IBM Cloud offers a range of services and tools that can help you implement your disaster recovery plan effectively. Consult IBM's documentation and support resources for specific guidance and best practices.

For example, the following are all data plane responsibilities:

Running and hosting the Virtual Server Instance (VSI)

Reading and writing to block storage volumes

Getting and setting objects into Cloud Object Storage Buckets

Running, processing queries and updates to IBM Cloud Databases PostegreSQL database.

Listing the Virtual Server Instance instances (VSI) in the account and provisioning a new the Virtual Server Instance (VSI) orchestrating the creation of virtual machines from an OS image, block storage creation, attachment and configuration of the network endpoints

Configuring, resizing, and mounting block storage volumes

Creating new Cloud Object Storage Buckets.

The global platform services use global load-balancing strategies to ensure a redundant, highly available platform is available for you to access and manage your cloud services.

What is a disaster recovery plan and how does it work?

A disaster recovery plan (DR or DRP) is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber attacks and any other disruptive events. The plan contains strategies to minimize the effects of a disaster, so an organization can continue to operate or quickly resume key operations.

Disruptions can lead to lost revenue, brand damage and dissatisfied customers — and the longer the recovery time, the greater the adverse business impact. Therefore, a good disaster recovery plan should enable rapid recovery from disruptions, regardless of the source of the disruption.

A DR plan is more focused than a business continuity plan and does not necessarily cover all contingencies for business processes, assets, human resources and business partners.

A successful DR solution typically addresses all types of operation disruption and not just the major natural or man-made disasters that make a location unavailable. Disruptions can include power outages, telephone system outages, temporary loss of access to a facility due to bomb threats, a “possible fire” or a low-impact non-destructive fire, flood or other event. A DR plan should be organized by type of disaster and location. It must contain scripts (instructions) that can be implemented by anyone.

Before the 1970s, most organizations only had to concern themselves with making copies of their paper-based records. Disaster recovery planning gained prominence during the 1970s as businesses began to rely more heavily on computer-based operations. At that time, most systems were batch-oriented mainframes. Another offsite mainframe could be loaded from backup tapes, pending recovery of the primary site.

In 1983 the U.S. government mandated that national banks must have a testable backup plan. Many other industries followed as they understood the significant financial losses associated with long-term outages.

By the 2000s, businesses had become even more dependent on digital online services. With the introduction of big data, cloud, mobile and social media, companies had to cope with capturing and storing massive amounts of data at an exponential rate. DR plans had to become much more complex to account for much larger amounts of data storage from a myriad of devices. The advent of cloud computing in the 2010s helped to alleviate this disaster recovery complexity by allowing organizations to outsource their disaster recovery plans and solutions.

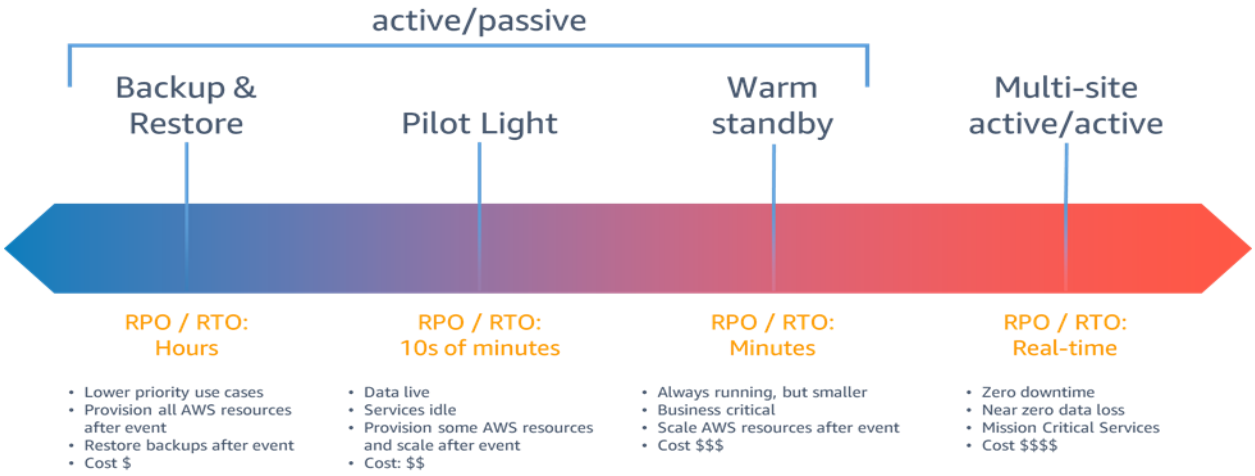
Another current trend that emphasizes the importance of a detailed disaster recovery plan is the increasing sophistication of cyber attacks. Industry statistics show that many attacks stay undetected for well over 200 days. With so much time to hide in a network, attackers can plant malware that finds its way into the backup sets –infecting even recovery data. Attacks may stay dormant for weeks or months, allowing malware to propagate throughout the system. Even after an attack is detected, it can be extremely difficult to remove malware that is so prevalent throughout an organization.

Business disruption due to a cyber attack can have a devastating impact on an organization. For instance, cyber outage at a package delivery company can disrupt operations across its supply chain, leading to financial and reputational loss. In today's digitally dependent world, every second of that disruption counts.

Why is a disaster recovery plan important?

The compelling need to drive superior customer experience and business outcome is fueling the growing trend of hybrid multicloud adoption by enterprises. Hybrid multicloud, however, creates infrastructure complexity and potential risks that require specialized skills and tools to manage. As a result of the complexity, organizations are suffering frequent outages and system breakdown, coupled with cyber-attacks, lack of skills, and supplier failure. The business impact of outages or unplanned downtime is extremely high, more so in a hybrid multicloud environment. Delivering resiliency in a hybrid multicloud requires a disaster recovery plan that includes specialized skills, an integrated strategy and advanced technologies, including orchestration for data protection and recovery. Organizations must have comprehensive enterprise resiliency with orchestration technology to help mitigate business continuity risks in hybrid multicloud, enabling businesses to achieve their digital transformation goals.

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are two of the most important parameters of a disaster recovery or data protection plan. These are objectives that can guide enterprises to choose an optimal cloud backup and disaster recovery plan.



The RPO/RTO, along with a business impact analysis, provides the basis for identifying, analyzing, and explaining viable strategies for inclusion in the business continuity plan. Viable strategRecovery Point Objective (RPO) is the maximum acceptable amount of time since the last data recovery

Point. This objective determines what is considered an acceptable loss of data between the last recovery

Point and the interruption of service and is defined by the organization.

Limit of what they can spend on their data recovery strategy. Of the four DR strategies, either Pilot Lighty options include any which would enable resumption of a business process in a time frame at or near the RPO/RTO.